MAR 7 1931

QA
1
J92

D13

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

Herausgegeben von

K. Hensel

H. Hasse L. Schlesinger

Wissenschaftlicher Beirat

H. Brandt / M. Dehn / G. Doetsch / A. Fraenkel / O. Haupt / F. Hausdorff
E. Hellinger / G. Kowalewski / H. Rademacher / K. Reidemeister
A. Rosenthal / C. Schaefer / W. Schmeidler / F. Schottky / O. Toeplitz

Band 164

Heft 1

Ausgegeben den 16. Februar 1931

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung — J. Guttentag, Verlagsbuchhandlung — Georg Reimer — Karl J. Trübner — Veit & Comp.

Berlin W 10 und Leipzig

1931

Band 164. Heft 1.

Inhaltsverzeichnis.

	Seite
Artin, E., Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper	1
Krull, Wolfgang, Zur Arithmetik der Potenzreihen mit ganzzahligen Koeffizienten	12
— — Eine Bemerkung über rationalzahlige Potenzreihen	23
Karamata, J., Neuer Beweis und Verallgemeinerung der Tauberschen Sätze, welche die Laplacesche und Stieltjessche Transformation betreffen	27
Mordell, L. J., The condition for integer solutions of $ax^3+by^3+cz^3+dt^3=0$ . .	40
Haupt, Otto, Über die Struktur reeller Kurven	50
Korselt, A., Einfacher Beweis eines Satzes von Kronecker	61
Franz, Wolfgang, Zur vorstehenden Arbeit von Herrn A. Korselt	63
Löbell, Frank, Gewindebüschel und ihre Invarianten	64

An unsere Mitarbeiter!

Es ist unbedingt notwendig, daß alle zur Einsendung gelangenden Manuskripte sowohl vollkommen druckfertig, als auch in gut lesbarer, möglichst Maschinen-Schrift gehalten sind, wobei die gotischen und griechischen wie überhaupt alle besonderen Typen durch Buntstift bezeichnet werden. Nachträgliche Korrekturen verursachen wesentliche Kosten, die sich naturgemäß auf die Preisgestaltung des Journals mit auswirken müssen. Machen sich also aus irgend einem Grunde Text-Änderungen eines Beitrages notwendig, so sind diese der Schriftleitung sofort mitzuteilen, wenn sie die endgültige Annahme und Weitergabe an den Verlag meldet; Korrekturen nach dem Vorliegen des Satzes dürfen sich ausschließlich auf die Verbesserung von Satzfehlern erstrecken.

Manuskripte, die den eingangs erwähnten Vorschriften entsprechen, ermöglichen auch der Schriftleitung eine raschere Prüfung als schwer leserliche und können infolgedessen schneller zum Druck gelangen.

Im Interesse des schnellen Erscheinens der einzelnen Hefte erhalten die Herren Verfasser grundsätzlich nur eine Korrektur ihrer Beiträge. Da seitens der Schriftleitung die Korrekturen in typographischer Hinsicht sorgfältige Lesung finden und die richtige Ausführung der Autor-Korrekturen genau überwacht wird, hoffen wir, auch so allen Wünschen gerecht zu werden.

Die Herren Verfasser erhalten von Abhandlungen bis zu 24 Seiten Umfang 100 Sonderabdrucke, von größeren Arbeiten 50 Sonderabdrucke kostenfrei, weitere gegen Berechnung.

Sendungen für das Journal erbittet die Redaktion ausschließlich unter der Adresse:

An die Redaktion des Journals für die reine und angewandte Mathematik

Professor Dr. Kurt Hensel, Marburg (Bez. Cassel), Behringweg 7.

Die gruppentheoretische Struktur der Diskriminanten algebraischer Zahlkörper.

Von *E. Artin* in Hamburg.

Zwischen der Relativdiskriminante eines relativ abelschen Körpers und den Führern der Klassenkörpertheorie besteht eine enge Beziehung. Die Kenntnis der Relativdiskriminanten aller Zwischenkörper zieht die Kenntnis der Führer dieser Körper nach sich und umgekehrt. Vermittelt wird dieser Zusammenhang durch die Führer-Diskriminanten-Formel, deren Beweis entweder analytisch mit Hilfe der Funktionalgleichung der L-Reihen geführt wird oder, wie Herr Hasse kürzlich gezeigt hat, der Normenrestheorie entnommen werden kann [1]). Man wird nun erwarten, daß sich Strukturs ätze dieser Art auch im allgemeinen galoisschen Fall beweisen lassen. Da wir bis heute über die Zerlegungsgesetze in nicht-abelschen Körpern nichts wissen, kann ein solcher Einblick nur in formaler Weise erfolgen.

Wir werden zeigen, daß sich jedem Charakter der Gruppe eines galoisschen Körpers ein Ideal des Grundkörpers zuordnen läßt und daß dann die Diskriminante eines jeden Zwischenkörpers sich aus diesen „Führern“ in ähnlicher Weise aufbaut, wie im abelschen Fall. Ist die Gruppe abelsch, so stimmen diese Ideale mit den Führern der Charaktere im gewöhnlichen Sinn überein. Im allgemeinen Fall spielen sie in der Funktionalgleichung der L-Reihen mit Frobenius-Charakteren die gleiche Rolle, wie die Führer im abelschen Fall [2]). Man wird daher mit Recht erwarten, daß auch im Fall nicht-abelscher Gruppen unsere Ideale eine ausgezeichnete Rolle bei den Zerlegungsgesetzen spielen werden. Doch vermag ich über diese Frage nichts auszusagen.

Immerhin scheinen mir diese Erwägungen die Wichtigkeit der neuen Begriffe für die künftige Entwicklung der algebraischen Zahlentheorie zu zeigen. Man wird vielleicht hinter das Geheimnis der Zerlegungsgesetze kommen, wenn man die Ergebnisse dieser Arbeit direkt zu begründen sucht. Der Sachverhalt ist nämlich dieser:

Sieht man ab von der Tatsache, daß unsere Ideale im abelschen Fall die „wirklichen“ Führer sind (hier braucht man natürlich die Klassenkörpertheorie), so lassen sich alle übrigen Sätze elementar beweisen, bis auf die Tatsache, daß unsere Führer ganze Ideale des Grundkörpers sind; dieser letzte Einblick läßt sich vorläufig nur mit Hilfe der Klassenkörpertheorie gewinnen. Ich kann aber nicht daran glauben, daß diese dazu wirklich erforderlich ist. Ein Beweis könnte zum Beispiel dadurch erbracht werden,

[1]) Vgl. H. Hasse, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil I, Jahresbericht der deutschen Mathematikervereinigung **35** (1926), Satz 16. Teil I a dieses Berichts in Bd. **36** (1927) gibt auch in § 8 eine Begründung der in dieser Arbeit verwendeten Begriffe aus der Theorie der galoisschen Körper. Ferner: H. Hasse, Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper, ds. Journal **162** (1930).

[2]) E. Artin, Zur Theorie der L-Reihen mit allgemeinen Gruppencharakteren, Hamburger Abhandlungen 8 (1931). Die in Teil II des in Anm. 1 zitierten Berichts von Herrn Hasse, Ergänzungsband **6** (1930), Seite 193, aufgeführten Probleme über L-Reihen haben zu der vorliegenden Untersuchung den Anstoß gegeben.

daß man die Kongruenzen (15) entsprechend verallgemeinert. Mehr noch verspricht allerdings die folgende Erwägung:

Die Diskriminante eines Zwischenkörpers gestattet eine Zerlegung in Faktoren, die so aussieht, wie wenn die Diskriminante als Gruppendeterminante geschrieben werden könnte. Vielleicht kann sie in der Tat so geschrieben werden und vielleicht kann man das direkt einsehen. Aus einer solchen Schreibweise würde man alle Sätze dieser Arbeit ablesen können. Ich bin aber auch davon überzeugt, daß man aus einer solchen Schreibweise die unbekannten Zerlegungsgesetze erraten könnte. Doch muß das alles der künftigen Entwicklung vorbehalten bleiben.

Es sei noch gestattet darauf hinzuweisen, daß die explizite Formel für die Führer der Charaktere auch eine neue Ergänzung zur Klassenkörpertheorie darstellt.

1. Hilfsätze.

1. Zwischen den einfachen Charakteren $\chi_i(\sigma)$ einer Gruppe $\mathfrak{G}$ und den einfachen Charakteren $\psi_k(\sigma)$ einer Untergruppe $\mathfrak{U}$ bestehen bekanntlich Relationen, die von Frobenius [3]) herrühren:

Setzt man fest, daß unter $\psi_k(\sigma)$ der Wert 0 zu verstehen ist, wenn σ nicht in der Untergruppe $\mathfrak{U}$ liegt, durchläuft ferner τ_i ein volles Repräsentantensystem der rechtsseitigen Nebengruppen von $\mathfrak{U}$ nach $\mathfrak{G}$, so ist die Funktion

$$\chi_{\psi_k}(\sigma) = \sum_i \psi_k(\tau_i \sigma \tau_i^{-1}) \tag{1}$$

ein (im allgemeinen nicht einfacher) Charakter der Gruppe $\mathfrak{G}$. Ist

$$\chi_{\psi_k}(\sigma) = \sum_{i=1}^{h} r_{ik}\, \chi_i(\sigma), \qquad k = 1, 2, \ldots, l \tag{2}$$

seine Darstellung durch die $\chi_i(\sigma)$, so gilt umgekehrt für die $\chi_i(\sigma)$ innerhalb der Untergruppe $\mathfrak{U}$ die Darstellung:

$$\chi_i(\sigma) = \sum_{k=1} r_{ik}\, \psi_k(\sigma), \qquad \sigma \text{ aus } \mathfrak{U},\ i = 1, 2, \ldots, h. \tag{3}$$

Für die Zahlen r_{ik} findet man:

$$r_{ik} = \frac{1}{q} \sum_{\tau \text{ aus } \mathfrak{U}} \chi_i(\tau)\, \psi_k(\tau^{-1}). \tag{4}$$

In diesen Formeln bedeuten n, q die Ordnungen, h, l die Anzahl der Charaktere von $\mathfrak{G}$ und $\mathfrak{U}$. $\chi_{\psi_k}(\sigma)$ heißt der von $\psi_k(\sigma)$ induzierte Charakter.

Ist $\chi(\sigma)$ ein Charakter von $\mathfrak{G}$, so ist jede konjugiert algebraische Funktion auch ein Charakter. Die Summe eines Systems konjugiert algebraischer Charaktere ist ein Charakter, der nur ganz rationaler Werte fähig ist und rationaler Charakter genannt werde. Ist i eine zu n teilerfremde Zahl, so ist die Funktion $\chi(\sigma^i)$ aus der Funktion $\chi(\sigma)$ zu erhalten, indem man in dem Ausdruck von $\chi(\sigma)$ als Spur die n-te Einheitswurzel durch ihre i-te Potenz ersetzt, also zu einem konjugiert algebraischen Charakter übergeht. Daraus folgt, daß die rationalen Charaktere $\Xi_k(\sigma)$ der Gleichung genügen:

$$\Xi_k(\sigma^i) = \Xi_k(\sigma), \qquad (i, n) = 1. \tag{5}$$

Sie sind also lediglich Funktionen der sogenannten Abteilungen der Gruppe.

Die von einem Element ϱ aus $\mathfrak{G}$ erzeugte Untergruppe werde mit $\mathfrak{U}^\varrho$ bezeichnet. Um diese verschiedenen Untergruppen zu unterscheiden, denken wir uns in den vorigen Formeln, soweit erforderlich, noch einen oberen Index ϱ angebracht. Ferner verabreden wir, daß dem Hauptcharakter einer Gruppe immer die Nummer 1 entsprechen soll. Ins-

[3]) G. Frobenius, Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen, Sitzungsberichte Berlin 1898. Ferner: A. Speiser, Gruppentheorie, 1. Aufl. (1923) § 52 oder 2. Aufl. (1927) § 62.

besondere setzen wir in Formel (2) für k den Wert 1 ein. Dann steht links ein rationaler Charakter. Die Darstellungen durch die einfachen Charaktere sind eindeutig, so daß also auf der rechten Seite konjugiert algebraische Charaktere die gleichen Koeffizienten r_{ik}^{ϱ} erhalten. Faßt man also konjugiert algebraische Charaktere immer zusammen, so erhält man eine Formel der Gestalt:

$$\chi_{\psi_i \varrho}(\sigma) = \sum_{i=1}^{h'} R_i^{\varrho} \Xi_i(\sigma). \tag{6}$$

Dabei sind die $\Xi_i(\sigma)$ die aus den einfachen Charakteren gewonnenen rationalen Charaktere, h' ihre Anzahl und R_i^{ϱ} einer der alten Koeffizienten r_{i1}^{ϱ} in neuer Nummerierung. Summiert man in (4) über ein System konjugiert algebraischer Charaktere $\chi_i(\tau)$ so findet man, wenn p_i angibt, wieviel einfache Charaktere in $\Xi_i(\sigma)$ stecken, für R_i^{ϱ} den Ausdruck:

$$R_i^{\varrho} = \frac{1}{q^{\varrho} p_i} \sum_{\nu=1}^{q^{\varrho}} \Xi_i(\varrho^{\nu}). \tag{7}$$

Wir lassen nun in (6) das Element ϱ die ganze Gruppe $\mathfrak{G}$ durchlaufen und erhalten so ein System linearer Gleichungen für die als unbekannt zu betrachtenden rationalen Charaktere. Behauptet wird, daß es lösbar ist. Die Matrix des Gleichungssystems lautet (R_i^{ϱ}), wo i etwa die Nummer der Zeile, ϱ die Nummer der Spalte angibt. Die Lösbarkeit des Systems ist garantiert, wenn sich darunter h' linear unabhängige Gleichungen, d. h. in der Matrix h' linear unabhängige Spalten vorfinden. Dies ist sicher der Fall, wenn die h' Zeilen der Matrix linear unabhängig sind. Sei also

$$\sum_{i=1}^{h'} R_i^{\varrho} x_i = 0, \quad \varrho \text{ aus } \mathfrak{G}, \tag{8}$$

eine lineare Relation zwischen den Zeilen der Matrix. Wir setzen (7) darin ein, lassen den unwesentlichen Faktor q^{ϱ} fort und ersetzen x_i durch das gleichwertige Produkt $x_i p_i$. So erhält man die Relation:

$$\sum_{\nu=1}^{q^{\varrho}} \sum_{i=1}^{h'} \Xi_i(\varrho^{\nu}) x_i = 0 \quad \text{für alle } \varrho \text{ aus } \mathfrak{G}. \tag{9}$$

Es gilt aber sogar:

$$\sum_{i=1}^{h'} \Xi_i(\varrho) x_i = 0 \qquad \text{für alle } \varrho \text{ aus } \mathfrak{G}. \tag{10}$$

Für das Einheitselement von $\mathfrak{G}$ folgt dies direkt aus (9). Nimmt man an, daß (10) bewiesen ist für alle Elemente kleinerer Ordnung als q^{ϱ}, so bleiben in (9) nur solche Summanden stehen, bei denen ν teilerfremd zu q^{ϱ} ist. Diese liegen aber alle in derselben Abteilung wie ϱ, die rationalen Charaktere haben für diese Potenzen also denselben Wert wie für ϱ, so daß jetzt (10) für ϱ folgt.

(10) würde besagen, daß die Ξ_i linear abhängig sind, falls auch nur ein $x_i \neq 0$ ist. Das geht nicht, denn die Ξ_i sind aus lauter verschiedenen einfachen Charakteren zusammengesetzt. Damit ist die Lösbarkeit des Systems (16) bewiesen. Wir benötigen aber nur das folgende, etwas schwächere Resultat:

Jeder rationale Charakter ist rationalzahlige Linearkombination von Charakteren, die ihrerseits von Hauptcharakteren von Untergruppen induziert sind.

2. Wir gehen jetzt zu arithmetischen Betrachtungen über. Als Grundkörper k werde irgendein algebraischer Zahlkörper genommen. K sei galoissch über k, $\mathfrak{G}$ seine Gruppe, Ω sei ein Zwischenkörper und $\mathfrak{U}$ die zugehörige Untergruppe. $\mathfrak{p}$ sei ein Primideal aus k. Wir verwenden die folgenden Bezeichnungen:

$\mathfrak{p} = \mathfrak{q}_1^{e_1} \mathfrak{q}_2^{e_2} \cdots \mathfrak{q}_s^{e_s}$ sei die Zerlegung von $\mathfrak{p}$ in Ω.

$\mathfrak{P}_i$ sei ein Primteiler von $\mathfrak{q}_i$ in K und zwar sei $\mathfrak{P}_i = \varkappa_i \mathfrak{P}_1$, wobei $\varkappa_i$ Element von $\mathfrak{G}$ sei. $\mathfrak{P}_i^{e'_i}$ sei die höchste Potenz von $\mathfrak{P}_i$ die in $\mathfrak{q}_i$ aufgeht, es werde $e = e_i e'_i$ gesetzt, so daß e die höchste Potenz von $\mathfrak{P}_i$ ist, die in $\mathfrak{p}$ aufgeht. f_i und f seien die Relativgrade von $\mathfrak{q}_i$ und $\mathfrak{P}_i$ in bezug auf k, f'_i derjenige von $\mathfrak{P}_i$ in bezug auf Ω. $\mathfrak{Z}$ und $\mathfrak{T}$ seien Zerlegungs- bzw. Trägheitsgruppe von $\mathfrak{P}_1$ in bezug auf k, so daß $\mathfrak{Z}_i = \varkappa_i \mathfrak{Z} \varkappa_i^{-1}$ und $\mathfrak{T}_i = \varkappa_i \mathfrak{T} \varkappa_i^{-1}$ die entsprechenden Gruppen von $\mathfrak{P}_i$ sind. Der Durchschnitt irgendeiner Gruppe mit $\mathfrak{U}$ werde durch Überstreichen gekennzeichnet. Dann sind also $\overline{\mathfrak{Z}}_i$ und $\overline{\mathfrak{T}}_i$ die entsprechenden Gruppen von $\mathfrak{P}_i$ in bezug auf Ω. σ_i sei eine dem Primteiler $\mathfrak{P}_i$ zugeordnete Frobenius-Substitution in bezug auf k und ϱ_i eine Frobenius-Substitution dieses Primteilers in bezug auf Ω. Diese Substitutionen erzeugen die zugehörigen Zerlegungsgruppen $\mathfrak{Z}_i$ bezw. $\overline{\mathfrak{Z}}_i$.

Die absolute Norm irgendeines Primideals in irgendeinem Körper möge einheitlich immer mit N bezeichnet werden, da Mißverständnisse nicht zu befürchten sind. Aus der Bedeutung der Frobenius-Substitutionen σ_i und ϱ_i folgen dann die Kongruenzen:

$$\sigma_i^{f_i} \mathsf{A} \equiv \mathsf{A}^{Nq_i} \pmod{\mathfrak{P}_i} \text{ und } \varrho_i^{-1} \mathsf{A}^{Nq_i} \equiv \mathsf{A} \pmod{\mathfrak{P}_i}, \text{ also } \varrho_i^{-1} \sigma_i^{f_i} \mathsf{A} \equiv \mathsf{A} \pmod{\mathfrak{P}_i}$$

für jedes ganze A aus K. Die letzte Kongruenz besagt, daß $\varrho_i^{-1} \sigma_i^{f_i}$ in $\mathfrak{T}_i$ liegt, daß also $\sigma_i^{f_i} \mathfrak{T}_i = \varrho_i \mathfrak{T}_i$ ist. Nun ist $\mathfrak{T}_i$ ein Normalteiler von $\mathfrak{Z}_i$ und σ_i und ϱ_i gehören zu dieser letzteren Gruppe. Also folgt auch: $\sigma_i^{\nu f_i} \mathfrak{T}_i = \varrho_i^{\nu} \mathfrak{T}_i$. Daraus schließen wir, daß in der Nebengruppe $\sigma_i^{\nu f_i} \mathfrak{T}_i$ ein Element aus $\mathfrak{U}$ liegt, nämlich ϱ_i^{ν}.

Wir wollen uns nun umgekehrt fragen, wann in der Nebengruppe $\sigma_i^{\mu} \mathfrak{T}_i$ ein Element $\gamma = \sigma_i^{\mu} \tau_i$ aus $\mathfrak{U}$ liegt. Dann gilt für alle ganzen A von K die Kongruenz:

$$\gamma \mathsf{A} \equiv \mathsf{A}^{Np^{\mu}} \pmod{\mathfrak{P}_i}.$$

Wählen wir für A insbesondere ein Element aus Ω, für das ja $\gamma \mathsf{A} = \mathsf{A}$ ist, so folgt:

$$\mathsf{A} \equiv \mathsf{A}^{Np^{\mu}} \pmod{\mathfrak{q}_i}.$$

Die Existenz einer Primitivwurzel mod $\mathfrak{q}_i$ zeigt dann, daß μ durch f_i teilbar sein muß, womit wir auf den vorhin behandelten Fall zurückgekommen sind. Es gilt dann: $\sigma_i^{\mu} \mathfrak{T}_i = \varrho_i^{\frac{\mu}{f_i}} \mathfrak{T}_i$. Damit nun $\varrho_i^{\frac{\mu}{f_i}} \tau_i$ in $\mathfrak{U}$ liegt, muß τ_i in $\mathfrak{U}$ also in $\overline{\mathfrak{T}}_i$ liegen. Zusammengefaßt hat sich ergeben:

Der Durchschnitt von $\sigma_i^{\mu} \mathfrak{T}_i$ mit $\mathfrak{U}$ ist leer, wenn μ nicht durch f_i teilbar ist; er besteht aus $\varrho_i^{\frac{\mu}{f_i}} \overline{\mathfrak{T}}_i$, wenn μ durch f_i teilbar ist.

Betrachten wir zwei Nebengruppen der Form $\mathfrak{U} \zeta_i \varkappa_i$ und $\mathfrak{U} \zeta'_k \varkappa_k$, wo ζ_i aus $\mathfrak{Z}_i$ und ζ'_k aus $\mathfrak{Z}_k$ stammt. Wann sind sie gleich? Das Element $\gamma = \zeta'_k \varkappa_k \varkappa_i^{-1} \zeta_i^{-1}$ muß zu $\mathfrak{U}$ gehören. Nun sieht man aber sofort, daß es das Primideal $\mathfrak{P}_i$ in $\mathfrak{P}_k$ überführt. Da nun ein Element aus $\mathfrak{U}$ einen Primteiler von $\mathfrak{q}_i$ nur wieder in einen Primteiler von $\mathfrak{q}_i$ überführen kann, folgt zunächst $i = k$. Jetzt ist $\gamma = \zeta'_i \zeta_i^{-1}$. Der Form nach liegt dieses Element in $\mathfrak{Z}_i$; da es zu $\mathfrak{U}$ gehören soll, muß es in $\overline{\mathfrak{Z}}_i$ liegen. Will man also lauter verschiedene Nebengruppen erhalten, so hat man ζ_i ein volles Restsystem von $\mathfrak{Z}_i$ modulo $\overline{\mathfrak{Z}}_i$ durchlaufen zu lassen. Die Ordnung von $\mathfrak{Z}_i$ ist ef, die von $\overline{\mathfrak{Z}}_i$ ist $e'_i f'_i$, der Index von $\mathfrak{Z}_i$ nach $\overline{\mathfrak{Z}}_i$ demnach $e_i f_i$. Bezeichnet man also mit $\zeta_{i\nu}$ dieses volle Restsystem, so sind die Nebengruppen

$$\mathfrak{U} \zeta_{i\nu} \varkappa_i, \qquad i = 1, 2, \ldots, s; \quad \nu = 1, 2, \ldots, e_i f_i,$$

voneinander verschieden. Ihre Anzahl beträgt $\sum_{i=1}^{s} e_i f_i$, ist also der Körpergrad von Ω in bezug auf k, d. h. der Index von $\mathfrak{G}$ nach $\mathfrak{U}$. Folglich sind dies gerade alle Nebengruppen,

und wir können das System $\zeta_{iv}\varkappa_i$ dazu benützen, den induzierten Charakter mit Hilfe von Formel (1) zu bilden. Sei also ψ irgendein Charakter von $\mathfrak{U}$. Dann gilt:

$$\chi_\psi(\lambda) = \sum_{i=1}^{s} \sum_{v=1}^{e_i f_i} \psi(\zeta_{iv}\varkappa_i \lambda \varkappa_i^{-1} \zeta_{iv}^{-1}). \tag{11}$$

Wir wollen im Argument eines Charakters auch Komplexe von Gruppenelementen einsetzen und verstehen darunter in naheliegender Weise die Summe der einzelnen Charakterwerte. Dann gilt die Formel (11) auch dann, wenn λ ein Komplex ist. Aus ihr leiten wir jetzt mehrere Formeln ab:

Zunächst werde unter λ der Komplex $\sigma_1^g \mathfrak{T}$ verstanden. Im Argument der rechten Seite wird er mit $\varkappa_i$ und mit ζ_{iv} transformiert. Die erste Transformation führt ihn in $\sigma_i^g \mathfrak{T}_i$ über, die zweite verändert dieses Resultat nicht mehr, da $\mathfrak{T}_i$ Normalteiler von $\mathfrak{Z}_i$ mit zyklischer Faktorgruppe ist und ζ_{iv} zu $\mathfrak{Z}_i$ gehört. Man erhält somit:

$$\chi_\psi(\sigma_1^g \mathfrak{T}) = \sum_{i=1}^{s} \sum_{v=1}^{e_i f_i} \psi(\sigma_i^g \mathfrak{T}_i) = \sum_{i=1}^{s} e_i f_i \; \psi(\sigma_i^g \mathfrak{T}_i).$$

Nun ist aber der Wert der Funktion ψ gleich 0, wenn das Argument nicht zu $\mathfrak{U}$ gehört. Wir dürfen also noch auf der rechten Seite die Durchschnitte der Argumente mit $\mathfrak{U}$ bilden. Aus den oben bestimmten Durchschnitten folgt jetzt:

$$\chi_\psi(\sigma_i^g \mathfrak{T}) = \sum_{f_i \mid g} e_i f_i \; \psi(\varrho_i^{\frac{g}{f_i}} \overline{\mathfrak{T}_i}). \tag{12}$$

Zweitens sei $\mathfrak{V}$ irgendein Normalteiler von $\mathfrak{Z}$. Für λ werde in Formel (11) $\mathfrak{V}$ eingesetzt. Bezeichnen wir die Gruppe $\varkappa_i \mathfrak{V} \varkappa_i^{-1}$ mit $\mathfrak{V}_i$ und beachten, daß auch sie Normalteiler von $\mathfrak{Z}_i$ wird, so folgt, daß die Argumente auf der rechten Seite die Werte $\mathfrak{V}_i$ haben. Die Durchschnittbildung führt analog wie früher auf die Formel:

$$\chi_\psi(\mathfrak{V}) = \sum_{i=1}^{s} e_i f_i \; \psi(\overline{\mathfrak{V}_i}). \tag{13}$$

Setzen wir endlich in Formel (1) $\sigma = 1$ und verstehen unter m den Index von $\mathfrak{G}$ nach $\mathfrak{U}$ also den Grad des Körpers Ω in bezug auf k, so folgt:

$$\chi_\psi(1) = m \; \psi(1). \tag{14}$$

Die Formel (12) wird in dieser Arbeit keine Verwendung finden. Wir haben sie hier gleich mit hergeleitet, da sie gut in diesen Zusammenhang paßt. In einer weiteren Arbeit werde ich ihren Nutzen zeigen [4]).

Noch einige Worte über die Bedeutung der Werte $\chi(\mathfrak{V})$. Es sei $\mathfrak{V}$ irgendeine Untergruppe von $\mathfrak{G}$ und v ihre Ordnung. Der Charakter χ von $\mathfrak{G}$ ist auch Charakter von $\mathfrak{V}$. Zerlegt man ihn in einfache Charaktere von $\mathfrak{V}$ und beachtet die Relationen für die Charaktere, so zeigt sich, daß $\frac{1}{v}\chi(\mathfrak{V})$ eine ganze rationale, nicht negative Zahl ist, die angibt, wie oft im Charakter χ der Hauptcharakter von $\mathfrak{V}$ steckt. Insbesondere ist der Wert von $\chi(\mathfrak{V})$ stets höchstens $v\chi(1)$ und dann und nur dann gleich dieser Zahl, wenn die zu χ gehörige Darstellung der Gruppe $\mathfrak{G}$ für jedes Element von $\mathfrak{V}$ die Einheitsmatrix liefert.

3. Als letzten Hilfssatz brauchen wir noch Beziehungen zwischen der Trägheitsgruppe und den Verzweigungsgruppen. Ein Teil dieses Hilfssatzes ist schon von Herrn Speiser gewonnen worden [5]).

Die i-te Verzweigungsgruppe des Primideals $\mathfrak{P}_1$ werde mit $\mathfrak{V}_i$ bezeichnet. Π sei

---

[4]) Siehe Anm. 2.

[5]) A. Speiser, Die Zerlegungsgruppe, ds. Journal **149** (1919).

eine genau durch die erste Potenz von $\mathfrak{P}_1$ teilbare Zahl von K. τ sei ein beliebiges Element der Trägheitsgruppe, und es führe Π über in $A\Pi$, wo A teilerfremd zu $\mathfrak{P}_1$ ausfällt. τ_i sei ein Element der i-ten Verzweigungsgruppe, lasse also Π modulo $\mathfrak{P}_1^{i+1}$ fest. Seine Wirkung nach dem Modul $\mathfrak{P}_1^{i+2}$ sei durch die Kongruenz

$$\tau_i \Pi \equiv \Pi + \Pi^{i+1} B \pmod{\mathfrak{P}_1^{i+2}}$$

beschrieben. Wegen

$$\tau_i A \equiv A \pmod{\mathfrak{P}_1^{i+1}}$$

folgt

$$\tau_i(A\Pi) \equiv A\tau_i\Pi \equiv A\Pi + (A\Pi)^{i+1}\frac{B}{A^i} \pmod{\mathfrak{P}_1^{i+2}}.$$

Wegen

$$\tau^{-1}(A\Pi) = \Pi \quad \text{und} \quad \tau^{-1}\left(\frac{B}{A^i}\right) \equiv \frac{B}{A^i} \pmod{\mathfrak{P}_1}$$

ist

$$\tau^{-1}\tau_i\tau\Pi \equiv \Pi + \Pi^{i+1}\frac{B}{A^i} \pmod{\mathfrak{P}_1^{i+2}}.$$

Daraus folgt endlich:

$$\tau_i^{-1}\tau^{-1}\tau_i\tau\Pi \equiv \Pi + \Pi^{i+1}B\left(\frac{1}{A^i} - 1\right) \pmod{\mathfrak{P}_1^{i+2}}.$$

Das Element $\tau_i^{-1}\tau^{-1}\tau_i\tau$ liegt also dann und nur dann in $\mathfrak{V}_{i+1}$, wenn entweder $B \equiv 0 \pmod{\mathfrak{P}_1}$ oder $A^i \equiv 1 \pmod{\mathfrak{P}_1}$ ist. Nehmen wir an, daß τ_i nicht zu $\mathfrak{V}_{i+1}$ gehört, daß also $B \not\equiv 0 \pmod{\mathfrak{P}_1}$ und somit $A^i \equiv 1 \pmod{\mathfrak{P}_1}$ ist, so muß demnach $\tau^i\Pi \equiv A^i\Pi \equiv \Pi \pmod{\mathfrak{P}_1^2}$ sein, also τ^i in $\mathfrak{V}_1$ liegen. Wir haben also:

Das Element $\tau_i^{-1}\tau^{-1}\tau_i\tau$ liegt dann und nur dann in $\mathfrak{V}_{i+1}$, wenn entweder τ_i zu $\mathfrak{V}_{i+1}$ oder τ^i zu $\mathfrak{V}_1$ gehört.

Als Nebenresultat erhalten wir sofort den Satz von Speiser:
Die Gruppe $\mathfrak{V}_i/\mathfrak{V}_{i+1}$ liegt im Zentrum der Gruppe $\mathfrak{V}_1/\mathfrak{V}_{i+1}$.

Wir benutzen aber unser Resultat dazu, Kongruenzen zwischen den Zahlen $\chi(\mathfrak{V}_i)$ herzuleiten. Die Trägheitsgruppe hat die Ordnung e. Zerlegen wir e in die Faktoren $e_0 p^{R_i}$, wo e_0 zu p teilerfremd und p die zum Primideal $\mathfrak{p}$ gehörige rationale Primzahl ist, so ist bekanntlich die Faktorgruppe $\mathfrak{T}/\mathfrak{V}_1$ zyklisch vor den Ordnung e_0. Unter τ werde jetzt ein Vertreter der erzeugenden Restklasse modulo $\mathfrak{V}_1$ verstanden.

Die Elemente τ_i aus $\mathfrak{V}_i$, die *nicht* in $\mathfrak{V}_{i+1}$ liegen, teilen wir jetzt in Klassen ein, indem wir alle Elemente der Form $\tau^{-\nu}\tau_i\tau^\nu$ in ein- und dieselbe Klasse legen. Die so gewonnenen Klassen sind fremd, und die Anzahl der Elemente einer Klasse ist jedesmal die kleinste Zahl k, so daß $\tau^{-k}\tau_i\tau^k = \tau_i$ ist. Erst recht ist dann $\tau_i^{-1}\tau^{-k}\tau_i\tau^k$ in $\mathfrak{V}_{i+1}$ enthalten, so daß τ^{ik} zu $\mathfrak{V}_1$ gehören muß. Die Zahl ik muß also durch e_0 teilbar sein. Ist nun χ ein Charakter, so haben alle Elemente derselben Klasse denselben Charakterwert, die Summe der Charakterwerte ist also eine durch k teilbare, ganze algebraische Zahl. Summieren wir jetzt über alle Klassen und multiplizieren noch mit i, so erhalten wir die Zahl $i(\chi(\mathfrak{V}_i) - \chi(\mathfrak{V}_{i+1}))$, deren Teilbarkeit durch e_0 somit feststeht. Es gilt also die Kongruenz:

$$i\chi(\mathfrak{V}_i) \equiv i\chi(\mathfrak{V}_{i+1}) \pmod{e_0}. \tag{15}$$

Wählen wir für χ den Hauptcharakter und bezeichnen wir die Ordnung von $\mathfrak{V}_i$ mit p^{R_i}, so ergibt sich der Spezialfall:

$$ip^{R_i} \equiv ip^{R_{i+1}} \pmod{e_0}. \tag{16}$$

Endlich werde $\mathfrak{G}$ als abelsch vorausgesetzt. Dann findet man:

Ist $\mathfrak{B}_{i+1}$ von $\mathfrak{B}_i$ verschieden, so ist i durch e_0 teilbar

Dieses Resultat ist auf anderem Wege von Herrn Hasse gewonnen worden[6]).

§ 2. Der Führer eines Charakters.

4. Wir geben jetzt die Definition des Führers eines Charakters im Relativkörper K/k:

$$\mathfrak{f}(\chi, K/k) = \prod_{\mathfrak{p}} \mathfrak{p}^{\frac{1}{e}[e\chi(1)-\chi(\mathfrak{T})+p^{R_1}\chi(1)-\chi(\mathfrak{B}_1)+p^{R_2}\chi(1)-\chi(\mathfrak{B}_2)+\cdots]}. \tag{17}$$

Dabei ist das Produkt über alle Primideale des Körpers k zu erstrecken[7]). Die auftretenden Zahlen und Gruppen sind schon erklärt worden. Da für genügend große Indizes die Verzweigungsgruppe nur aus dem Einheitselement besteht, bricht die Summe im Exponenten ab. Geht ferner das Primideal nicht in der Diskriminante auf, so besteht schon die Trägheitsgruppe nur aus dem Einheitselement, und das betreffende Primideal liefert keinen Beitrag zum Führer. (17) definiert uns also in der Tat ein Ideal. Aus der Bemerkung am Schlusse von 2 geht hervor, daß der Exponent eine nicht negative rationale Zahl ist und daß wenigstens der erste Bestandteil $\chi(1) - \frac{1}{e}\chi(\mathfrak{T})$ ganz rational ausfällt. Wir werden zeigen, daß der volle Exponent ganz rational ist, daß also $\mathfrak{f}(\chi, K/k)$ ein ganzes Ideal des Körpers k ist. Doch liegt diese Tatsache sehr tief. Vorläufig lassen wir es zu, daß der Führer möglicherweise nicht im Körper liegt und rechnen mit ihm in rein formaler Weise. Was dabei unter Norm zu verstehen ist, ist klar, möglicherweise ist aber die Norm auch kein Ideal des Körpers, in bezug auf den sie genommen wird.

Wir bestätigen sofort die Rechenregel:

$$\mathfrak{f}(\chi_1 + \chi_2, K/k) = \mathfrak{f}(\chi_1, K/k)\,\mathfrak{f}(\chi_2, K/k). \tag{18}$$

Zur Untergruppe $\mathfrak{U}$ gehöre wie bisher der Zwischenkörper Ω. Wir wollen die Beziehung zwischen den beiden Führern $\mathfrak{f}(\chi_\psi, K/k)$ und $\mathfrak{f}(\psi, K/\Omega)$ untersuchen.

Die Gruppe $\varkappa_\nu \mathfrak{B}_i \varkappa_\nu^{-1} = \mathfrak{B}_\nu^i$ ist die i-te Verzweigungsgruppe des Primideals $\mathfrak{P}_\nu$ in bezug auf k. Ihr Durchschnitt mit $\mathfrak{U}$ ist die i-te Verzweigungsgruppe in bezug auf Ω. Die Ordnung von $\overline{\mathfrak{B}}_\nu^i$ werde mit $p^{R_\nu^i}$ bezeichnet. Formel (13) liefert:

$$\chi_\psi(\mathfrak{B}_i) = \sum_{\nu=1}^{s} e_\nu f_\nu \psi(\overline{\mathfrak{B}}_\nu^i).$$

Das ergibt mit (14) und der Gleichung $m = \sum_{\nu=1}^{s} e_\nu f_\nu$ zusammen nach leichten Rechnungen die Umformung:

$$\begin{aligned}\mathfrak{p}^{\frac{1}{e}(p^{R_i}\chi_\psi(1)-\chi_\psi(\mathfrak{B}_i))} &= \mathfrak{p}^{\frac{m}{e}(p^{R_i}-1)\psi(1)} \cdot \mathfrak{p}^{-\frac{1}{e}\sum_{\nu=1}^{s} e_\nu f_\nu (p^{R_\nu^i}-1)\psi(1)} \cdot \mathfrak{p}^{\frac{1}{e}\sum_{\nu=1}^{s} e_\nu f_\nu (p^{R_\nu^i}\psi(1)-\psi(\overline{\mathfrak{B}}_\nu^i))} \\ &= N_{\Omega/k}\left(\mathfrak{p}^{\frac{1}{e}(p^{R_i}-1)\psi(1)} \cdot \prod_{\nu=1}^{s} \mathfrak{q}_\nu^{-\frac{1}{e'_\nu}(p^{R_\nu^i}-1)\psi(1)} \cdot \mathfrak{q}_\nu^{\frac{1}{e'_\nu}(p^{R_\nu^i}\psi(1)-\psi(\overline{\mathfrak{B}}_\nu^i))}\right).\end{aligned}$$

In ähnlicher Weise läßt sich auch der Beitrag der Trägheitsgruppe umformen. Nun haben die Relativdifferenten $\mathfrak{d}_{K/k}$ und $\mathfrak{d}_{K/\Omega}$ die Werte:

$$\mathfrak{d}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\frac{1}{e}(e-1+p^{R_1}-1+\cdots)}; \qquad \mathfrak{d}_{K/\Omega} = \prod_{\mathfrak{p}} \prod_{\nu=1}^{s} \mathfrak{q}_\nu^{\frac{1}{e'_\nu}(e'_\nu-1+p^{R_\nu^1}-1+p^{R_\nu^2}-1+\cdots)}.$$

Daraus folgt:

---

[6]) Vgl. die zweite der in Anm. 1 zitierten Arbeiten.

[7]) Damit die Formel überhaupt Sinn hat, muß man sich im Exponenten immer je zwei Glieder durch eine Klammer zusammengefaßt denken. Der Übersichtlichkeit halber wurden diese Klammern weggelassen.

$$\mathfrak{f}(\chi_\psi, K/k) = N_{\Omega/k}\left(\left(\frac{\mathfrak{d}_{K/k}}{\mathfrak{d}_{K/\Omega}}\right)^{\psi(1)} \cdot \prod_{\mathfrak{p}} \prod_{\nu=1}^{s} \mathfrak{q}_\nu^{\frac{1}{e'_\nu}(e'_\nu \psi(1) - \psi(\bar{\mathfrak{T}}_\nu) + p^{R^1_\nu}\psi(1) - \psi(\bar{\mathfrak{B}}^1_\nu) + \cdots)}\right).$$

Der letzte Teil in dieser Formel ist aber gerade der Führer $\mathfrak{f}(\psi, K/\Omega)$. Wir erhalten somit die folgende grundlegende Formel:

$$\mathfrak{f}(\chi_\psi, K/k) = \mathfrak{D}_{\Omega/k}^{\psi(1)} \cdot N_{\Omega/k}(\mathfrak{f}(\psi, K/\Omega)), \tag{19}$$

wo die Relativdiskriminante von Ω nach k mit $\mathfrak{D}_{\Omega/k}$ bezeichnet ist.

Ist χ der Hauptcharakter, so wird $\mathfrak{f}(\chi, K/k) = 1$. Dies benutzen wir, um einen besonders wichtigen Spezialfall von (19) aufzustellen. Wir setzen nämlich in (19) für ψ den Hauptcharakter ψ_1 ein und erhalten die folgende Formel:

$$\mathfrak{D}_{\Omega/k} = \mathfrak{f}(\chi_{\psi_1}, K/k). \tag{20}$$

Diese Formel liefert uns die gewünschte Zerfällung der Diskriminanten aller Unterkörper von K. Man kann ja in der Tat den induzierten Charakter durch die einfachen Charaktere der Gruppe ausdrücken und erhält so wegen (18) eine Darstellung der Diskriminante durch die Führer der einfachen Charaktere. Die Führer lassen sich also als eine Verfeinerung der Diskriminantentheorie betrachten.

Eine weitere, fast triviale Eigenschaft der Führer besteht darin, daß sie für konjugiert algebraische Charaktere die gleichen Werte annehmen.

Es ist nun sehr bemerkenswert, daß sich die Führer durch diese letzte Eigenschaft sowie durch die Formeln (18) und (20) kennzeichnen lassen:

Ist jedem Charakter χ der Gruppe $\mathfrak{G}$ ein Ideal $\mathfrak{F}(\chi)$ zugeordnet für das die Formeln (18) *und* (20) *gelten, und entsprechen konjugiert algebraischen Charakteren die gleichen Ideale, so ist das Ideal $\mathfrak{F}(\chi)$ gleich dem Führer $\mathfrak{f}(\chi, K/k)$.*

Setzen wir nämlich

$$\mathfrak{F}_1(\chi) = \frac{\mathfrak{F}(\chi)}{\mathfrak{f}(\chi, K/k)},$$

so gilt noch immer (18), während an Stelle von (20) die einfachere Gleichung

$$\mathfrak{F}_1(\chi_{\psi_1}) = 1$$

tritt. Auf Grund des in 1 bewiesenen Hilfssatzes, folgt jetzt auch für jeden rationalen Charakter Ξ die Gleichung $\mathfrak{F}_1(\Xi) = 1$. Nun entsteht aber aus dem Ideal $\mathfrak{F}_1(\chi)$ bereits durch Potenzieren ein Ideal der Form $\mathfrak{F}_1(\Xi)$, so daß jetzt für jeden Charakter gilt: $\mathfrak{F}_1(\chi) = 1$. Damit ist unser Satz bewiesen.

Von diesem Ergebnis werden wir zweimal Gebrauch machen.

Erstens denken wir uns den Körper K zu einem umfassenderen galoisschen Körper K' erweitert. Ist $\mathfrak{G}'$ die Gruppe von K'/k und gehört K zur Untergruppe $\mathfrak{H}$, so ist $\mathfrak{G}$ mit der Faktorgruppe $\mathfrak{G}'/\mathfrak{H}$ isomorph und kann gleich mit ihr identifiziert werden. Dabei müssen wir also die bisherigen Gruppenelemente als Nebengruppen betrachten. Jeder Charakter der Gruppe $\mathfrak{G}$ ist dann auch Charakter in der Gruppe $\mathfrak{G}'$ und soll im folgenden immer mit dem gleichen Buchstaben bezeichnet werden. Dies geht umso eher, als alle Charakterrelationen in $\mathfrak{G}'$ erhalten bleiben, auch die für den induzierten Charakter. Setzen wir nun für jeden Charakter von $\mathfrak{G}$:

$$\mathfrak{F}(\chi) = \mathfrak{f}(\chi, K'/k),$$

so gilt für dieses Ideal wieder (18) und (20), und es hat für konjugiert algebraische Charaktere den gleichen Wert. Es folgt somit:

$$\mathfrak{f}(\chi, K'/k) = \mathfrak{f}(\chi, K/k). \tag{21}$$

Die Bedeutung der Formel ist die, daß sich die Führer in einem tieferen Sinn als bisher als Invarianten des Körpers K erweisen.

Zweitens wollen wir annehmen, daß die Gruppe $\mathfrak{G}$ abelsch ist. Ist χ ein einfacher Charakter von $\mathfrak{G}$, so setzen wir $\mathfrak{F}(\chi)$ gleich dem Führer der Klassenkörpertheorie. Für zusammengesetzte Charaktere werde dann $\mathfrak{F}(\chi)$ so definiert, daß (18) gilt. Dann bedeutet (20) für unsere Funktion nichts anderes, als die Führer-Diskriminanten-Formel der Klassenkörpertheorie [8]). Daß $\mathfrak{F}(\chi)$ für konjugiert algebraische Charaktere den gleichen Wert hat, ist selbstverständlich. Also hat sich ergeben:

Ist K/k abelsch, so ist der Führer $\mathfrak{f}(\chi, K/k)$ der bekannte Führer der Klassenkörpertheorie.

Auf Grund dieser fundamentalen Tatsache hege ich die Hoffnung, daß $\mathfrak{f}(\chi, K/k)$ auch im nicht-abelschen Fall zu den noch unbekannten Zerlegungsgesetzen in einer analogen Beziehung stehen wird. Doch können wir heute über diese Dinge noch nichts aussagen.

5. Wir wenden uns jetzt der Frage zu, ob $\mathfrak{f}(\chi, K/k)$ ein ganzes Ideal von k ist. Da der Exponent schon als nicht negativ erkannt ist, hat man nur noch seine Ganzheit nachzuweisen. Wir müssen also zeigen, daß der Klammerausdruck durch e teilbar ist. Entsprechend der Zerlegung von e in $e_0 p^{R_1}$ gliedert sich dieser Nachweis in den der Teilbarkeit durch e_0 und den der Teilbarkeit durch p^{R_1}.

Wir beginnen mit der Teilbarkeit durch e_0 und ersetzen im Exponenten den Ausdruck $p^{R_i}\chi(1) - \chi(\mathfrak{V}_i)$ durch $i(p^{R_i}\chi(1) - \chi(\mathfrak{V}_i)) - (i-1)(p^{R_i}\chi(1) - \chi(\mathfrak{V}_i))$.
Fassen wir die Glieder des Klammerausdrucks anders zusammen, so entstehen lauter Glieder der Form $i(p^{R_i} - p^{R_{i+1}})$ und $i(\chi(\mathfrak{V}_i) - \chi(\mathfrak{V}_{i+1}))$. Wegen (15) und (16) sind diese Glieder durch e_0 teilbar, also auch der ganze Klammerausdruck.

Die Teilbarkeit durch p^{R_1} liegt anscheinend wesentlich tiefer. Der Nachweis zerfällt in drei Schritte:

a) Reduktion auf Gruppen von Primzahlpotenzordnung.

Es sei V der erste Verzweigungskörper, also der zur Untergruppe $\mathfrak{V}_1$ gehörige Unterkörper von K. $\mathfrak{q}$ sei dasjenige Primideal aus V, das durch $\mathfrak{P}_1$ teilbar ist. Um die Trägheitsgruppe sowie die Verzweigungsgruppen von K/V zu bilden, hat man den Durchschnitt von $\mathfrak{T}, \mathfrak{V}_1, \mathfrak{V}_2, \ldots$ mit $\mathfrak{V}_1$ zu suchen. Es ist also die neue Trägheitsgruppe $\mathfrak{V}_1$, wogegen sich an den Verzweigungsgruppen nichts ändert. Die Ordnung der neuen Trägheitsgruppe ist gerade p^{R_1}. Nun ist χ auch Charakter der Untergruppe $\mathfrak{V}_1$. Wir bilden jetzt den Führer $\mathfrak{f}(\chi, K/V)$ und vergleichen den Beitrag des Primideals $\mathfrak{q}$ mit dem Beitrag von $\mathfrak{p}$ zu $\mathfrak{f}(\chi, K/k)$. Der Beitrag von $\mathfrak{q}$ lautet:

$$\frac{1}{p^{R_1}}\left(p^{R_1}\chi(1) - \chi(\mathfrak{V}_1) + p^{R_1}\chi(1) - \chi(\mathfrak{V}_1) + p^{R_2}\chi(1) - \chi(\mathfrak{V}_2) + \cdots\right).$$

Die ersten beiden Summanden sind dabei belanglos, da sie ohnehin ganz sind. Wenn wir zeigen könnten, daß $\mathfrak{f}(\chi, K/V)$ ein ganzes Ideal von V ist, so würde auch die Teilbarkeit des alten Klammerausdrucks durch p^{R_1} folgen, da ja die Exponenten in den wesentlichen Punkten übereinstimmen. $\mathfrak{V}_1$ aber ist eine Gruppe der Ordnung p^{R_1}.

b) Wir können also annehmen, daß $\mathfrak{G}$ eine Gruppe von Primzahlpotenzordnung ist. Nach einem Satz von Blichfeldt [9]) ist dann jede Darstellung der Gruppe eine monomiale, es ist also jeder Charakter induziert von einem Charakter ersten Grades einer

[8]) Siehe Anm. 1. χ_{ψ_1} gehört zur regulären Darstellung von $\mathfrak{G}/\mathfrak{U}$, enthält also jeden einfachen Charakter von $\mathfrak{G}/\mathfrak{U}$ genau einmal.

[9]) A. Speiser, Gruppentheorie, 1. Aufl. Satz 130 oder 2. Aufl. Satz 169. Eine ähnliche Anwendung dieses Satzes hat Herr Hasse im zweiten Teil seines in Anm. 1 zitierten Berichts, Ergänzungsband 6 (1930), Seite 160, gegeben.

geeigneten Untergruppe. Sei ψ der Charakter der Untergruppe und Ω der zur Untergruppe gehörige Zwischenkörper. Wir können jetzt Formel (19) anwenden und sehen: Wenn $\mathfrak{f}(\psi, K/\Omega)$ ein ganzes Ideal des Körpers Ω ist, so ist auch $\mathfrak{f}(\chi, K/k)$ ein Ideal aus k.

c) Es ist also die weitere Annahme erlaubt, daß es sich bei χ um einen Charakter ersten Grades handelt. Jeder solche Charakter aber ist schon Charakter einer zyklischen Faktorgruppe und Formel (21) lehrt, daß wir die Gruppe $\mathfrak{G}$ als zyklische Gruppe annehmen dürfen. Wir stützen uns nun auf die Klassenkörpertheorie. Wir wissen nämlich, daß dann $\mathfrak{f}(\chi, K/k)$ mit dem Führer der Klassenkörpertheorie übereinstimmt. Also ist unser Ideal selbstverständlich ein Ideal des Körpers.

Damit ist gezeigt:

Das Ideal $\mathfrak{f}(\chi, K/k)$ *ist ein ganzes Ideal aus* k.

Durch diesen Satz gewinnen die vorigen Resultate überhaupt erst Bedeutung, da man jetzt erst erkennt, daß es sich in der Tat um Aufspaltungen der Diskriminanten im Körper selbst handelt.

Wir führen noch die folgende Redeweise ein:

Ist der Charakter χ für keinen echten galoisschen Unterkörper Charakter, so wollen wir sagen, daß der Führer $\mathfrak{f}(\chi, K/k)$ *genau* zu K gehört.

Im Führer $\mathfrak{f}(\chi, K/k)$ können nur die Teiler der Diskriminante von K/k aufgehen. Gehört $\mathfrak{f}(\chi, K/k)$ aber genau zu K, so gehen alle Diskriminantenteiler auch wirklich auf. Da nämlich keiner der Beiträge $\frac{1}{e}(p^{R_i}\chi(1) - \chi(\mathfrak{V}^i))$ negativ ist, kann $\mathfrak{p}$ nur dann nicht in $\mathfrak{f}(\chi, K/k)$ aufgehen, wenn insbesondere $e\chi(1) - \chi(\mathfrak{T}) = 0$ ist. Aus der Bemerkung am Schlusse von 2 folgt jetzt, daß die zu χ gehörige Darstellung sich für jedes Element von $\mathfrak{T}$ auf eine Einheitsmatrix reduzieren muß. Nun bilden aber die Elemente von $\mathfrak{G}$, für die das eintritt, einen Normalteiler von $\mathfrak{G}$ und χ ist Charakter für die Faktorgruppe dieses Normalteilers. Nach unserer Voraussetzung muß sich also diese Gruppe auf das Einheitselement reduzieren, und ein gleiches gilt für die Gruppe $\mathfrak{T}$. Also geht $\mathfrak{p}$ nicht in der Diskriminante von K/k auf. Es sei gestattet, die bisher gefundenen Eigenschaften noch einmal übersichtlich zusammenzustellen:

Das Ideal

$$\mathfrak{f}(\chi, K/k) = \prod_{\mathfrak{p}} \mathfrak{p}^{\frac{1}{e}[e\chi(1) - \chi(\mathfrak{T}) + p^{R_1}\chi(1) - \chi(\mathfrak{V}_1) + p^{R_2}\chi(1) - \chi(\mathfrak{V}_2) + \cdots]} \tag{17}$$

ist ein ganzes Ideal aus k. *Ist* K/k *abelsch, so ist es der Führer der Klassenkörpertheorie. Gehört es genau zu* K/k, *so ist es durch alle Diskriminantenteiler und nur durch diese teilbar. Es gelten die Formeln:*

$$\mathfrak{f}(\chi_1 + \chi_2, K/k) = \mathfrak{f}(\chi_1, K/k)\,\mathfrak{f}(\chi_2, K/k), \tag{18}$$

$$\mathfrak{f}(\chi_\psi, K/k) = \mathfrak{D}_{\Omega/K}^{\psi(1)} \cdot N_{\Omega/k}(\mathfrak{f}(\psi, K/\Omega)), \tag{19}$$

$$\mathfrak{f}(\chi, K/k) = \mathfrak{f}(\chi, K'/k), \quad \textit{wenn } K' \textit{ Oberkörper von } K \textit{ ist.} \tag{21}$$

Die Diskriminante eines Zwischenkörpers gewinnt man mit Hilfe der Formel:

$$\mathfrak{D}_{\Omega/k} = \mathfrak{f}(\chi_{\psi_1}, K/k) \tag{20}$$

oder, wenn $\chi_{\psi_1} = \sum_{\nu=1}^{h} g_\nu \chi_\nu$ *die Zerlegung von* χ_{ψ_1} *in einfache Charaktere bedeutet,*

$$\mathfrak{D}_{\Omega/k} = \prod_{\nu=1}^{h} (\mathfrak{f}(\chi_\nu, K/k))^{g_\nu} \tag{20a}$$

(χ_{ψ_1} *ist einfach der Charakter der Permutationsgruppe zu der* Ω *gehört*). *Speziell:*

$$\mathfrak{D}_{K/k} = \prod_{\nu=1}^{h} (\mathfrak{f}(\chi_\nu, K/k))^{\chi_\nu(1)}. \tag{20b}$$

Wir können jetzt auch leicht einige Minkowskische Sätze über Diskriminanten auf die Führer übertragen.

6. Wählen wir als Grundkörper den Körper der rationalen Zahlen, so geht im Führer sicher mindestens eine Primzahl auf, wenn χ nicht der Hauptcharakter ist. Denn ist K' der Körper zu dem $\mathfrak{f}(\chi)$ genau gehört, so geht in der Diskriminante von K' mindestens eine Primzahl auf.

Ist der Grundkörper k beliebig, bedeutet $\mathfrak{f}$ ein gegebenes Ideal und n eine gegebene ganze rationale Zahl, so kann man nach allen Körpern K/k fragen, zu denen $\mathfrak{f}$ als Führer genau gehört, wobei wir den Grad von K auf n festlegen. Da wir die Diskriminantenteiler von K/k als die Teiler von $\mathfrak{f}$ kennen gelernt haben, können wir nun mit Hilfe von Satz 80 des Hilbertschen Zahlberichtes schließen, daß für die Diskriminante nur endlich viele Möglichkeiten in Frage kommen. Zu gegebener Relativdiskriminante und gegebenem Grade gibt es aber nach Minkowski nur endlich viele Körper. Damit ist bewiesen:

Ist $\mathfrak{f}$ ein gegebenes Ideal aus k, so gibt es nur endlich viele relativ galoissche Oberkörper festen Grades, zu denen $\mathfrak{f}$ als Charakter genau gehören kann. Ist der Grundkörper insbesondere der Körper der rationalen Zahlen, so kann die Zahl 1 *nur als Führer für den Hauptcharakter auftreten, gehört also genau nur zum Grundkörper selbst.*

Ohne Beweis sei wenigstens noch der Umstand erwähnt, daß der eben ausgesprochene Satz noch richtig bleibt, wenn man statt dem Körpergrade nur dem Grade des Charakters die Einschränkung auferlegt. Der Nachweis dieser Tatsache ist etwas umständlich.

Endlich weise ich noch darauf hin, daß ich in einer weiteren Arbeit zeigen werde, daß die Führer in der Theorie der L-Reihen mit allgemeinen Gruppencharakteren dieselbe Rolle spielen, wie bei L-Reihen mit abelschen Charakteren [10]).

[10]) Siehe Anm. 2.

Eingegangen 9. November 1930.

Zur Arithmetik der Potenzreihen mit ganzzahligen Koeffizienten.

Von *Wolfgang Krull* in Erlangen.

In einer unter dem gleichen Titel in der Mathematischen Zeitschrift erschienenen Arbeit hat J. Schur gezeigt, daß im Bereich $\mathfrak{O}$ aller formalen oder auch aller konvergenten Potenzreihen in x mit Koeffizienten aus der Hauptordnung $\mathfrak{o}$ eines endlichen algebraischen Zahlkörpers $\mathfrak{k}$ jedes Hauptideal eindeutig als Produkt von Primidealen darstellbar ist, und er hat zugleich in $\mathfrak{O}$ die Klasse derjenigen Ideale, die Faktoren von Hauptidealen sind — wir wollen diese Ideale für den Augenblick kurz als Quasihauptideale bezeichnen — genau charakterisiert [1]). Dagegen gibt die Schursche Arbeit keine allgemeine Auskunft auf die Frage nach dem besonderen Bau der unter den Quasihauptidealen von $\mathfrak{O}$ vorkommenden Primideale. Im folgenden soll nun diese Frage erschöpfend beantwortet werden. Dabei gehen wir im wesentlichen folgendermaßen vor:

Neben der Hauptordnung $\mathfrak{o}$ und ihrem Potenzreihenring $\mathfrak{O}$ betrachten wir die zu den einzelnen Primidealen $\mathfrak{p}$ von $\mathfrak{o}$ gehörigen Henselschen π-adischen Zahlringe $\mathfrak{o}_\mathfrak{p}$ [2]) und ihre Potenzreihenringe $\mathfrak{O}_\mathfrak{p}$. Es zeigt sich dann zunächst, daß die Untersuchung von $\mathfrak{O}$ vollständig zurückgeführt werden kann auf die Untersuchung der einzelnen $\mathfrak{O}_\mathfrak{p}$. Die Ringe $\mathfrak{O}_\mathfrak{p}$ hinwiederum können — und das ist der entscheidende Gedanke — genau so behandelt werden, wie die Potenzreihenringe in zwei Variabeln mit Körperkoeffizienten. Man braucht zu diesem Zwecke nur zu beachten, daß der Koeffizientenbereich $\mathfrak{o}_\mathfrak{p}$ sozusagen den Ring aller Potenzreihen in einem Primelement π mit Koeffizienten aus dem Restklassenkörper von $\mathfrak{o}_\mathfrak{p}$ nach π darstellt. Diese Auffassung ermöglicht insbesondere die Übertragung des von den Potenzreihen in zwei und mehr Variabeln mit Körperkoeffizienten her bekannten Weierstraßschen Vorbereitungssatzes auf die Ringe $\mathfrak{O}_\mathfrak{p}$, und daraus ergibt sich dann leicht alles für unsere Zwecke nötige, insbesondere eine genaue Charakterisierung der Primidealfaktoren der Hauptideale.

Als wichtiges Hilfsmittel beim Beweise des Weierstraßschen Vorbereitungssatzes für die $\mathfrak{O}_\mathfrak{p}$ und bei der Herstellung der Zusammenhanges zwischen $\mathfrak{O}$ und den einzelnen

[1]) Math. Zeitschrift 12 (1922), S. 95—113. In der Schurschen Arbeit, die in Zukunft kurz mit S. zitiert werden soll, ist neben dem Fall aller formalen und dem aller konvergenten Potenzreihen auch noch der Fall behandelt, daß $\mathfrak{O}$ aus allen und nur den Potenzreihen besteht, die rationale Funktionen darstellen. Die Methoden der vorliegenden Arbeit sind ihrer Natur nach wohl auf die beiden ersten Möglichkeiten, nicht aber auf die dritte anwendbar; denn es ist unmittelbar klar, daß im dritten Fall die Primidealfaktoren der Hauptideale von $\mathfrak{O}$ unmöglich auf die gleiche Weise charakterisiert werden können, wie im Fall eins und zwei. An S. habe ich schon einmal angeknüpft, und zwar in der folgenden, in Zukunft kurz mit K. zu zitierenden Note: Idealtheorie der Potenzreihen einer Variabeln mit ganzen algebraischen Zahlkoeffizienten. Beiträge zur Algebra 3. Sitz. Ber. d. Heildelberger Akademie d. Wissenschaften, Math. Nat. Klasse 1927, 8. Abhandl.

[2]) Zur Theorie der π-adischen Zahlen vgl. etwa: K. Hensel, Eine neue Theorie der algebraischen Zahlen, Math. Zeitschrift 2 (1918), S. 433—452.

$\mathfrak{O}_\mathfrak{p}$ dient uns ein allgemeiner Satz über die Möglichkeit der Normierung einer Potenzreihe durch Multiplikation mit einem geeigneten Einheitsfaktor. Ich habe diesen Satz, den „Normierungshilfssatz", wegen seiner vielfachen Verwendbarkeit in § 1 in ganz allgemeiner Fassung ausführlich bewiesen.

Überhaupt habe ich die Untersuchung möglichst allgemein geführt, und insbesondere als Koeffizientenbereich der Potenzreihen nicht die Hauptordung $\mathfrak{o}$ eines endlichen algebraischen Zahlkörpers und ihre zugehörigen π-adischen Ringe $\mathfrak{o}_\mathfrak{p}$, sondern einen beliebigen „Multiplikationsring" $\mathfrak{m}$ und seine zugehörigen $\mathfrak{p}$-adischen Ringe $\mathfrak{m}_\mathfrak{p}$ gewählt. Dadurch wurde ein kurzes Eingehen auf die allgemeine Theorie der Multiplikationsringe nötig. Im übrigen aber verläuft die Untersuchung keineswegs umständlicher als im Spezialfall algebraischer Koeffizienten, und es läßt sich sogar gerade vom allgemeinen Standpunkt aus die Klasse der Quasihauptideale besonders einfach und naturgemäß charakterisieren.

Die Ergebnisse der vorliegenden Arbeit können fast unmittelbar auf Potenzreihen in mehreren Veränderlichen übertragen werden, wenn man sich auf die Betrachtung von solchen Hauptidealen beschränkt, deren Basiselemente ein von 0 verschiedenes von den Variabeln freies Glied besitzen, und wenn man außerdem als Koeffizientenbereiche nur solche Multiplikationsringe zuläßt, bei denen die Restklassensysteme nach den verschiedenen Primidealen sämtlich unendlich viel verschiedene Elemente enthalten. (Dieser Bedingung genügen die Hauptordnungen der endlichen algebraischen Zahlkörper nicht; wohl aber genügen ihr die zu diesen Hauptordnungen gehörigen Kroneckerschen Funktionalringe sowie die Hauptordnungen der endlichen algebraischen Funktionenkörper.)

Dagegen reichen unsere Methoden, auch bei einschränkenden Voraussetzungen über den Koeffizientenbereich, nicht aus, wenn die Produktzerlegungen von ganz beliebigen Hauptidealen in Potenzreihenringen mehrerer Variabler untersucht werden sollen, eine Frage, die meines Wissens überhaupt noch nicht befriedigend beantwortet ist. Ich habe dieses Mißstandes halber auch die oben erwähnte, an und für sich leicht mögliche Verallgemeinerung unserer Ergebnisse auf spezielle Hauptideale in Potenzreihenringen mehrerer Variabler im Texte nicht mehr weiter berücksichtigt.

Vorbemerkungen zur Terminologie.

Wir benutzen die in der allgemeinen Idealtheorie üblichen Bezeichnungen und Abkürzungen. Unter „Ring" oder „Integritätsbereich" verstehen wir stets einen kommutativen Ring ohne Nullteiler mit Einheitselement 1. Das Nullideal schließen wir ein für allemal von der Betrachtung aus. Wenn nichts besonders bemerkt ist, verstehen wir unter Ideal schlechtweg stets ein „*ganzes*" *Ideal* also ein Ideal, das Untermenge des Ringes ist, zu dem es gehört. Doch werden wir es, vor allem in § 3, auch mit „*gebrochenen*" *Idealen* zu tun haben; dabei bedeutet „gebrochenes Ideal des Ringes $\mathfrak{R}$" einen bel. $\mathfrak{R}$-Modul aus dem zu $\mathfrak{R}$ gehörigen Quotientenkörper $\mathfrak{K}$, der nur die Eigenschaft besitzen soll, durch Multiplikation mit einem geeigneten Hauptideal in ein ganzes Ideal verwandelt werden zu können. Ist $\mathfrak{a}$ ein (ganzes) Ideal aus dem Integritätsbereich $\mathfrak{R}$, so bezeichnen wir mit $\mathfrak{R} \mid \mathfrak{a}$ den Restklassenring von $\mathfrak{R}$ nach $\mathfrak{a}$, während wir unter einem „*vollen Restsystem von* $\mathfrak{R}$ *nach* $\mathfrak{a}$" eine Untermenge $\mathfrak{r}$ von $\mathfrak{R}$ verstehen, die aus jeder Restklasse von $\mathfrak{R} \mid \mathfrak{a}$ genau einen Repräsentanten enthält.

Ist der Ring $\mathfrak{R}$ Obermenge des Ringes $\mathfrak{S}$ und bedeutet $\mathfrak{a}_\mathfrak{s}$ ein Ideal aus $\mathfrak{S}$, so versteht man unter dem *Erweiterungsideal* von $\mathfrak{a}_\mathfrak{s}$ hinsichtlich $\mathfrak{R}$ das Modulprodukt $\mathfrak{R} \cdot \mathfrak{a}_\mathfrak{s}$, also das mengentheoretisch kleinste Ideal aus $\mathfrak{R}$, das sämtliche Elemente von $\mathfrak{a}_\mathfrak{s}$ enthält; umgekehrt definiert man zu jedem Ideal $\mathfrak{a}_\mathfrak{r}$ aus $\mathfrak{R}$ das *Verengungsideal* hinsichtlich $\mathfrak{S}$ als den mengen-

theoretischen Durchschnitt $\mathfrak{a}_r \frown \mathfrak{S}$ von $\mathfrak{a}_r$ und $\mathfrak{S}$. Als *Zurückleitungsideal* von $\mathfrak{a}_s$ hinsichtlich $\mathfrak{R}$ bzw. von $\mathfrak{a}_r$ hinsichtlich $\mathfrak{S}$ schließlich bezeichnen wir das Ideal $(\mathfrak{a}_s \cdot \mathfrak{R}) \frown \mathfrak{S}$ bzw. $(\mathfrak{a}_r \frown \mathfrak{S}) \cdot \mathfrak{R}$. — Das Zurückleitungsideal eines Ideals $\mathfrak{a}_s$ bezw. $\mathfrak{a}_r$ aus $\mathfrak{S}$ bzw. $\mathfrak{R}$ hinsichtlich $\mathfrak{R}$ bzw. $\mathfrak{S}$ ist sicher eine Obermenge von $\mathfrak{a}_s$ bzw. eine Untermenge von $\mathfrak{a}_r$. Es seien ferner S und R zwei Scharen von Idealen aus $\mathfrak{S}$ und $\mathfrak{R}$, die beide gleichzeitig mit zwei Idealen stets auch deren Produkt enthalten, und zwischen denen folgende Beziehungen bestehen: a) Das Erweiterungsideal eines Ideals aus S hinsichtlich $\mathfrak{R}$ gehört zu R, das Verengungsideal eines Ideals aus R hinsichtlich $\mathfrak{S}$ gehört zu S. b) Jedes Ideal aus S bzw. R ist mit seinem Zurückleitungsideal hinsichtlich $\mathfrak{R}$ bzw. $\mathfrak{S}$ identisch. Dann kann man zwischen den Idealbereichen S und R eine eindeutig umkehrbare und hinsichtlich der Teilbarkeitsverhältnisse und der Produktbildung isomorphe Beziehung dadurch herstellen, daß man jedem Ideal aus S sein Erweiterungsideal hinsichtlich $\mathfrak{R}$, jedem Ideal aus R sein Verengungsideal hinsichtlich $\mathfrak{S}$ zuordnet. Wir wollen in diesem Falle die *Idealbereiche R und S* kurz *äquivalent* nennen [3]).

§ 1. Perfektheit hinsichtlich eines Primideals. Der Normierungshilfssatz.

Der Integritätsbereich $\mathfrak{J}$ soll *hinsichtlich des Primideals* $\mathfrak{p}$ perfekt heißen, wenn ein unendliches Kongruenzsystem $x \equiv a_i (\mathfrak{p}^i)$ nach sämtlichen Potenzen von $\mathfrak{p}$ in $\mathfrak{J}$ stets eine und nur eine Lösung hat, falls nur die a_i der „Verträglichkeitsbedingung" $a_{i+1} \equiv a_i (\mathfrak{p}^i)$ $(i = 1, 2, \ldots)$ genügen [4]).

Einheitenhilfssatz. *Ist $\mathfrak{J}$ hinsichtlich $\mathfrak{p}$ perfekt, so ist das Element e dann und nur dann in $\mathfrak{J}$ Einheit, wenn e modulo $\mathfrak{p}$ Einheit, d. h. wenn die Kongruenz $e \cdot x \equiv 1 (\mathfrak{p})$ in $\mathfrak{J}$ lösbar ist.*

Das „nur dann" ist trivial. Zum Beweise des „dann" braucht man wegen der Perfektheitsvoraussetzung nur zu zeigen: Aus der Existenz einer Lösung e_1 von $e \cdot x \equiv 1 (\mathfrak{p})$ ergibt sich die Existenz einer Folge $e_1, e_2, \ldots$, die der Verträglichkeitsbedingung genügt, und bei der für e_i jeweils die Kongruenz $e \cdot e_i \equiv 1 (\mathfrak{p}^i)$ gilt. Induktion! Es seien $e_1, e_2, \ldots, e_n$ bereits gefunden, dann gilt eine Gleichung $e \cdot e_n = 1 + p_n$, $p_n \equiv 0 (\mathfrak{p}^n)$, und wenn wir $e_{n+1} = e_n - e_1 \cdot p_n$ setzen, wird $e_{n+1} \equiv e_n (\mathfrak{p}^n)$, $e \cdot e_{n+1} = e \cdot e_n - e \cdot e_1 \cdot p_n \equiv 1 (\mathfrak{p}^{n+1})$. Ist das Primideal $\mathfrak{p}$, hinsichtlich dessen $\mathfrak{J}$ perfekt ist, ein Hauptideal (p), so besitzt jedes unendliche Kongruenzsystem $x \equiv \sum_{i=1}^{n} a_i p^{i-1} (\mathfrak{p}^n)$ $(n = 1, 2, \ldots)$ in $\mathfrak{J}$ eine einzige Lösung a, und wir können und wollen geradezu $a = a_1 + a_2 p + a_3 p^2 + \cdots$ setzen und von einer „*Potenzreihenentwicklung von a nach p*" reden. Ist $\mathfrak{R}$ ein volles Restsystem von $\mathfrak{J}$ nach $\mathfrak{p}$, so besitzt, wie leicht einzusehen, jedes Element a eine Potenzreihenentwicklung $a = \sum_{i=1}^{\infty} a_i p^{i-1}$, bei der die Koeffizienten a_i sämtlich zu $\mathfrak{R}$ gehören.

Normierungshilfssatz. *Es sei $\mathfrak{J}$ hinsichtlich des Primideals $\mathfrak{p} = (p)$ perfekt, ferner sei e Einheit, $a \not\equiv 0 (\mathfrak{p})$, $a_0^* \equiv a \cdot e (\mathfrak{p})$; schließlich bedeute $\mathfrak{r}$ ein volles Restsystem von $\mathfrak{J}$ nach dem Ideal $(p, a) = (p, a_0^*)$. Dann gibt es in $\mathfrak{J}$ eine und nur eine Einheit e^*, für die das Produkt $a \cdot e^* = a^*$ eine Potenzreihenentwicklung $a^* = a_0^* + a_1^* p + a_2^* p^2 + \cdots$ besitzt, bei der $a_1^*, a_2^*, \ldots$ alle zu $\mathfrak{r}$ gehören.*

Aus $a \not\equiv 0 (\mathfrak{p})$, $a \cdot e \equiv a_0^* (\mathfrak{p})$ ergibt sich, daß e^* der Kongruenz $e^* \equiv e (\mathfrak{p})$ genügen, und daher sicher Einheit sein muß. Um die Existenz und Eindeutigkeit von e^* nachzu-

[3]) Vgl. hierzu: H. Grell, Beziehungen zwischen den Idealen verschiedener Ringe, Math. Annalen 97 (1927), S. 490—523, § 3.

[4]) Das Wort „perfekt" habe ich gewählt, um auf einen Zusammenhang mit der Bewertungstheorie hinzuweisen. Ist nämlich $\mathfrak{p} = (p)$ ein Hauptideal und stellt $\mathfrak{J}|\mathfrak{p}$ einen Körper dar, so besagt unsere Perfektheitsdefinition nichts anderes, als daß $\mathfrak{J}$ dann und nur dann hinsichtlich $\mathfrak{p}$ perfekt heißen soll, wenn der Quotientenkörper von $\mathfrak{J}$ hinsichtlich der mit Hilfe von $\mathfrak{p}$ zu definierenden diskreten Bewertung im Sinne der Bewertungstheorie perfekt ist.

weisen, setzen wir für e^* eine Potenzreihenentwicklung $e^* = e + e_1^* p + e_2^* p^2 + \cdots$ an, und zeigen, daß die Koeffizienten $e_1^*, e_2^*, \ldots$ in $\mathfrak{R}$ nacheinander eindeutig so bestimmt werden können, daß für $i = 1, 2, \ldots$ jeweils eine Kongruenz $a \cdot (e + e_1^* p + \cdots + e_{i-1}^* p^{i-1}) \equiv a_0^* + a_1^* p + \cdots + a_{i-1}^* p^{i-1} (\mathfrak{p}^i)$ gilt, bei der $a_1^*, a_2^*, \ldots, a_{i-1}^*$ alle zu $\mathfrak{r}$ gehören. Nehmen wir nun an, die Existenz und Eindeutigkeit von $e_1^*, \ldots, e_{n-1}^*$ sei bereits bewiesen, und es sei $a(e + e_1^* + \cdots + e_{n-1}^* p^{n-1}) \equiv a_0^* + a_1^* p + \cdots + a_{n-1}^* p^{n-1} + e p^n (\mathfrak{p}^{n+1})$, so muß e_n^* ersichtlich in $\mathfrak{R}$ so ausgewählt werden, daß $a \cdot e_n^* + e$ modulo $\mathfrak{p} = (p)$ einem Element a_n^* aus $\mathfrak{r}$ kongruent wird. Das kann aber wegen der Definition von $\mathfrak{r}$ auf eine und wegen der Unteilbarkeit von a durch $\mathfrak{p}$ auch nur auf eine Weise geschehen. Existenz und Eindeutigkeit der sämtlichen e_n^* ist somit durch Induktionsschluß gesichert. Aus der Perfektheit von $\mathfrak{J}$ hinsichtlich $\mathfrak{p}$ ergibt sich weiter, daß der formal angesetzten Potenzreihe $e + e_1^* p + e_2^* p^2 + \cdots$ in $\mathfrak{J}$ wirklich ein Element e^* entspricht, und aus der Art der Konstruktion von e^* folgt schließlich, daß $a \cdot e^* = a^*$ wirklich eine Normalform der im Hilfssatz geforderten Art darstellt.

§ 2. Potenzreihen mit $\mathfrak{p}$-adischen Koeffizienten.

Der Integritätsbereich $\mathfrak{i}_\mathfrak{p}$ soll als $\mathfrak{p}$-adischer Ring[5]) bezeichnet werden, wenn $\mathfrak{i}_\mathfrak{p}$ hinsichtlich eines Primideals $\mathfrak{p} = (p)$ perfekt ist, und wenn außerdem der Restklassenring $\mathfrak{i}_\mathfrak{p} | \mathfrak{p}$ einen Körper darstellt. Aus dem Einheitenhilfssatz ergibt sich sofort, daß in $\mathfrak{i}_\mathfrak{p}$ jedes durch $\mathfrak{p}$ unteilbare Element Einheit ist, und daraus folgt weiter:

In $\mathfrak{i}_\mathfrak{p}$ ist jedes Element einer eindeutig bestimmten Potenz des Primelements p äquivalent[6]), *es gibt also in $\mathfrak{i}_\mathfrak{p}$ außer $\mathfrak{i}_\mathfrak{p} = (p^0)$, $\mathfrak{p} = (p)$, $\mathfrak{p}^2 = (p^2)$, ... keine weiteren Ideale.* Das einfachste Beispiel eines $\mathfrak{i}_\mathfrak{p}$ ist der Ring $\mathfrak{J}_\mathfrak{p}$ aller (formalen) Potenzreihen in x mit Koeffizienten aus einem Körper $\mathfrak{k}$. ($\mathfrak{p} = (x)$). — Wir verstehen jetzt unter $\mathfrak{J}_\mathfrak{p}$ den Ring der Potenzreihen in x mit Koeffizienten aus dem $\mathfrak{p}$-adischen Integritätsbereich $\mathfrak{i}_\mathfrak{p}$. $\mathfrak{J}_\mathfrak{p}$ ist hinsichtlich der beiden Primideale (x) und (p) perfekt, und es ist $\mathfrak{J}_\mathfrak{p} | (x)$ zu $\mathfrak{i}_\mathfrak{p}$ isomorph. Betrachten wir ferner $\mathfrak{J}_\mathfrak{p} | (p)$! Bezeichnen wir mit $\bar{\mathfrak{i}}_\mathfrak{p}$ die Gesamtheit aller der Restklassen aus $\mathfrak{J}_\mathfrak{p} | (p)$, die Elemente aus $\mathfrak{i}_\mathfrak{p}$ enthalten, mit $\bar{x}$ die durch x bestimmte Restklasse, so ist $\bar{\mathfrak{i}}_\mathfrak{p}$ zu dem Körper $\bar{\mathfrak{k}} = \mathfrak{i}_\mathfrak{p} | \mathfrak{p}$ isomorph, und $\mathfrak{J}_\mathfrak{p} | (p)$ stellt den Ring der Potenzreihen in $\bar{x}$ mit Koeffizienten aus $\bar{\mathfrak{i}}_\mathfrak{p}$ dar, ist also vom Typus $\mathfrak{J}_\mathfrak{p}$. Daraus folgt durch Übergang von Gleichheiten in $\mathfrak{J}_\mathfrak{p} | (p)$ zu Kongruenzen modulo (p) in $\mathfrak{J}_\mathfrak{p}$ sofort:

Ist die Reihe $P = \sum_{i=0}^{\infty} a_i x^i$ aus $\mathfrak{J}_\mathfrak{p}$ modulo (p) genau durch x_m teilbar, d. h. ist a_m der erste durch $\mathfrak{p}$ unteilbare Koeffizient von P, so existiert in $\mathfrak{J}_\mathfrak{p}$ eine Reihe E, die modulo (p) und damit wegen des für $\mathfrak{J}_\mathfrak{p}$ gültigen Einheitenhilfssatzes auch absolut Einheit ist und der Kongruenz $P \cdot E \equiv x^m (p)$ genügt.

Ein Polynom $x^m + a_1 x^{m-1} + \cdots + a_m$ aus $\mathfrak{J}_\mathfrak{p}$, bei dem $a_1, a_2, \ldots, a_m$ alle durch $\mathfrak{p}$ teilbar sind, soll *Weierstraßsche Normalform* heißen. Das Produkt zweier Weierstraßschen Normalformen ist wieder eine Normalform, und es stellt das Polynom $x^n + b_1 x^{n-1} + \cdots + b_n$ aus $\mathfrak{J}_\mathfrak{p}$ sicher eine Weierstraßsche Normalform dar, wenn es Polynomfaktor einer derartigen Normalform ist.

Weierstraßscher Vorbereitungssatz. *Jede durch (p) unteilbare Reihe aus $\mathfrak{J}_\mathfrak{p}$ ist einer einzigen Weierstraßschen Normalform äquivalent.*

---

[5]) Das Wort „$\mathfrak{p}$-adisch" wurde gewählt, weil die Henselschen π-adischen Ringe neben den Potenzreihenringen $\mathfrak{J}_\mathfrak{p}$ des Textes die wichtigsten Spezialfälle des in Frage stehenden Ringtypus darstellen.

[6]) Zwei Ringelemente sollen äquivalent heißen, wenn sie sich nur um einen Einheitsfaktor unterscheiden.

Ist in der Reihe $P = \sum_{i=0}^{\infty} a_i x^i$ der Koeffizient a_m als erster durch (p) unteilbar, so müssen, wie leicht nachzurechnen, auch in jeder zu P äquivalenten Reihe $P \cdot E = \sum_{i=0}^{\infty} b_i x^i$ die Koeffizienten $b_0 b_1, \ldots, b_{m-1}$ durch $\mathfrak{p}$ teilbar sein, während b_m durch $\mathfrak{p}$ unteilbar ist. Daraus ergibt sich sofort, daß jede zu P etwa äquivalente Weierstraßsche Normalform als Polynom den Grad m besitzen muß, und das P zu keinen zwei verschiedenen Weierstraßschen Normalformen äquivalent sein kann, weil sonst P Potenzreihenfaktor eines nicht identisch verschwindenden Polynoms höchstens $(m-1)$-ten Grades wäre, was sicher ausgeschlossen ist. — Es bleibt noch zu zeigen, daß P überhaupt eine äquivalente Normalform besitzt. Wie bereits oben festgestellt, gilt eine Kongruenz $P \cdot E \equiv x^m (p)$ und es sind daher die Ideale (p, P) und (p, x^m) in $\mathfrak{J}_\mathfrak{p}$ identisch. Bedeutet ferner $\mathfrak{r}$ irgendein volles Restsystem von $\mathfrak{i}_\mathfrak{p}$ nach $\mathfrak{p}$, $\mathfrak{R}$ das System der Linearformen in $1, x, x^2, \ldots, x^{m-1}$ mit Koeffizienten aus $\mathfrak{r}$, so stellt $\mathfrak{R}$ offenbar ein volles Restsystem von $\mathfrak{J}_\mathfrak{p}$ nach $(\mathfrak{p}, x^m)$ dar. Wir können daher im Normierungshilfssatz $\mathfrak{J} = \mathfrak{J}_\mathfrak{p}$, $\mathfrak{p} = (p)$, $a = P$, $a_0^* = x^m$, $\mathfrak{r} = \mathfrak{R}$ setzen, und es ergibt sich, daß P in $\mathfrak{J}_\mathfrak{p}$ einer Reihe P^* äquivalent ist, die eine Potenzreihenentwicklung $P^* = x^m + \sum_{k=1}^{\infty} a_k^*(x)\, p^k$ nach p besitzt, bei der sämtliche $a_k^*(x)$ zu $\mathfrak{R}$ gehören. Ordnet man P^* nach Potenzen von x anstatt nach solchen von p, so entpuppt sich P^* als Weierstraßsche Normalform, und damit ist der nötige Existenzbeweis erbracht. Aus dem Weierstraßschen Vorbereitungssatz folgt jetzt leicht:

Satz 1. *In $\mathfrak{J}_\mathfrak{p}$ läßt sich jedes Element eindeutig*[7]) *als Produkt von Primelementen darstellen, d. h. es ist in $\mathfrak{J}_\mathfrak{p}$ jedes Hauptideal eindeutiges Produkt von solchen Primidealen, die selbst Hauptideale sind.*

Eine durch p unteilbare Reihe aus $\mathfrak{J}_\mathfrak{p}$ ist dann und nur dann Primelement, also Basis eines Primideals, wenn ihre zugehörige Weierstraßsche Normalform als Polynom im Koeffizientenring $\mathfrak{i}_\mathfrak{p}$ irreduzibel ist.

Da sich jede Reihe aus $\mathfrak{J}_\mathfrak{p}$ als Produkt einer eindeutig bestimmten Potenz des Primelements p mit einer durch p unteilbaren Reihe darstellen läßt, können wir uns beim Beweise auf die Betrachtung von solchen Reihen beschränken, die durch p unteilbar sind. Da ferner jede durch p unteilbare Reihe einer einzigen Weierstraßschen Normalform äquivalent ist, brauchen wir nur die Zerlegungen der Weierstraßschen Normalformen zu untersuchen. — Es sei also $P^* = P_1 \cdot P_2 \cdots P_s$ irgendeine Zerlegung der Normalform P^* im Ringe $\mathfrak{J}_\mathfrak{p}$. Dann müssen die P_i gleichzeitig mit P^* durch p unteilbar sein und somit Weierstraßsche Normalformen $P_i^* = E_i \cdot P_i$ besitzen; da ferner $P_1^* \cdot P_2^* \cdots P_s^* = (E_1 \cdot E_2 \cdots E_s) \cdot P^*$ offenbar eine zu P^* äquivalente Normalform darstellt, muß wegen der Eindeutigkeitsbehauptung des Weierstraßschen Vorbereitungssatzes die Gleichung $P^* = P_1^* \cdot P_2^* \cdots P_s^*$ gelten. Wir brauchen daher bei der Untersuchung von P^* nur solche Zerlegungen in Betracht zu ziehen, bei denen die Faktoren selbst Weierstraßsche Normalformen sind, und das heißt nichts anderes, als daß wir alle im Sinne der Teilbarkeit wesentlich verschiedenen Zerlegungen von P^* schon dann erhalten, wenn wir P^* als Polynom im Koeffizientenring $\mathfrak{i}_\mathfrak{p}$ auf alle möglichen Weisen zerlegen. Im Koeffizientenring $\mathfrak{i}_\mathfrak{p}$ aber läßt sich jedes Polynom nach dem sogenannten „Gaußschen Satz“ eindeutig in irreduzible Faktoren aufspalten, weil in $\mathfrak{i}_\mathfrak{p}$ jedes Element eindeutig als Produkt von Primele-

[7]) „Eindeutig“ bedeutet bei Zerlegungssätzen für Elemente natürlich nur „eindeutig bis auf Einheitsfaktoren“.

menten darstellbar ist. Aus unsern bisherigen Überlegungen ergibt sich daher, daß auch in $\mathfrak{J}_\mathfrak{p}$ jede Reihe eindeutig in Primelementfaktoren zerlegt werden kann. Es bleibt noch die Richtigkeit der in Satz 1 angegebenen Charakterisierung der Primelemente von $\mathfrak{J}_\mathfrak{p}$ nachzuweisen, und dazu haben wir nur zu zeigen: Eine Weierstraßsche Normalform P^* ist dann und nur dann als Polynom im Koeffizientenring $\mathfrak{i}_\mathfrak{p}$ nicht irreduzibel, also als Produkt von Faktoren niedrigeren Grades darstellbar, wenn sie auch in $\mathfrak{J}_\mathfrak{p}$ kein Primelement, also als Produkt von echten Teilern darstellbar ist. Was nun das „dann" der zu beweisenden Behauptung angeht, so folgt seine Richtigkeit unmittelbar aus den Betrachtungen, die zum Beweise des ersten Teils von Satz 1 führten. Das „nur dann" aber ergibt sich aus dem schon bereits früher hervorgehobenen Umstand, daß jeder Polynomfaktor einer Weierstraßschen Normalform vom Grade $m \geqq 1$ selbst (bis auf einen Fator aus $i_\mathfrak{p}$) eine Weierstraßsche Normalform, also sicher keine Einheit aus $\mathfrak{J}_\mathfrak{p}$ darstellt.

§ 3. Bemerkungen über Multiplikationsringe [8]).

Ein Integritätsbereich $\mathfrak{m}$ soll Multiplikationsring heißen, wenn in $\mathfrak{m}$ die Gesamtheit der ganzen und gebrochenen Ideale eine Gruppe hinsichtlich der Multiplikation darstellt. $\mathfrak{m}$ ist dann und nur dann Multiplikationsring, wenn im Bereich der ganzen Ideale von $\mathfrak{m}$ aus der Teilbarkeit von $\mathfrak{a}$ durch $\mathfrak{b}$ stets die Gültigkeit einer Gleichung $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$ folgt. Ist das beliebige Ideal $\mathfrak{a}$ aus $\mathfrak{m}$ Untermenge des Ideals $\mathfrak{b}$ so ist in der (wegen der Gruppeneigenschaft geltenden) Gleichung $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$ der Faktor $\mathfrak{c}$ ein ganzes Ideal [9]).

Ist der Integritätsbereich $\mathfrak{M}$ Obermenge des Multiplikationsrings $\mathfrak{m}$, so soll ein ganzes Ideal aus $\mathfrak{M}$ *Quasihauptideal* heißen, wenn es sich als Produkt eines ganzen Hauptideals von $\mathfrak{M}$ mit einem ganzen oder gebrochenen Ideal von $\mathfrak{m}$ darstellen läßt, $\mathfrak{Q} = \mathfrak{a} \cdot (A)$. Das Produkt zweier Quasihauptideale ist selbst ein Quasihauptideal, und aus der Gruppeneigenschaft der Ideale von $\mathfrak{m}$ folgt, leicht, daß jedes Quasihauptideal im Bereich der ganzen Ideale von $\mathfrak{M}$ von Faktor mindestens eines ganzen Hauptideals und damit nach bekannten Sätzen auch Faktor jedes Vielfachen ist [10]). *Sollen daher die Zerlegungsgesetze der Hauptideale in $\mathfrak{M}$ untersucht werden, so ist es zweckmäßig, von vornherein an Stelle der Klasse der Hauptideale die im allgemeinen größere Klasse der Quasihauptideale zu betrachten.*

Aus der Gruppeneigenschaft der Ideale von $\mathfrak{m}$ ergibt sich nach einer Bemerkung, die ich an anderer Stelle veröffentlicht habe, daß für die ganzen Ideale von $\mathfrak{m}$ der Noethersche Teilerkettensatz gilt [11]); und daraus folgt sofort, daß in $\mathfrak{m}$ jedes ganze Ideal

---

[8]) Vgl. auch: Krull, Über den Aufbau des Nullideals in ganz abgeschlossenen Ringen mit Teilerkettensatz (Math. Annalen **102** (1929), S. 363—369), § 3, wo auch Multiplikationsringe mit Nullteilern betrachtet werden.

[9]) Wir bezeichnen für beliebiges $\mathfrak{a}$ mit $\mathfrak{a}^{-1}$ das nach Voraussetzung existierende, der Gleichung $\mathfrak{a} \cdot \mathfrak{a}^{-1} = \mathfrak{m}$ genügende Ideal; dann ist $\mathfrak{a}^{-1}$ Obermenge von $\mathfrak{b}^{-1}$, falls $\mathfrak{a}$ Untermenge von $\mathfrak{b}$, und es muß mithin in der Gleichung $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$ des Textes $\mathfrak{c} = \mathfrak{a} \cdot \mathfrak{b}^{-1}$ Untermenge von $\mathfrak{m}$, d. h. ganz sein. Damit ist zugleich bewiesen, daß im Bereich der ganzen Ideale eines Multiplikationsrings tatsächlich aus der Teilbarkeit von $\mathfrak{a}$ durch $\mathfrak{b}$ stets die Gültigkeit einer Produktdarstellung $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{c}$ folgt. Um umgekehrt zu zeigen, daß ein Ring $\mathfrak{m}$ mit dieser letzten Eigenschaft immer ein Multiplikationsring ist, schließen wir so: Es sei $\mathfrak{a}$ ein beliebiges Ideal aus $\mathfrak{m}$; dann kann nach Definition der gebrochenen Ideale jedenfalls ein zweites Ideal $\mathfrak{b}$ so bestimmt werden, daß $\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{c}$ ganz ist. Bedeutet ferner (c) irgend ein durch $\mathfrak{c}$ teilbares Hauptideal, so gilt nach Voraussetzung eine Gleichung $\mathfrak{c} \cdot \mathfrak{d} = (c)$, und daraus folgt weiter $\mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{d} \cdot (c^{-1})) = \mathfrak{m}$. Zu beliebigem $\mathfrak{a}$ aus $\mathfrak{m}$ existiert also stets das reziproke Ideal $\mathfrak{a}^{-1}$, und daraus ergibt sich sofort die Gruppeneigenschaft des Bereichs aller Ideale von $\mathfrak{m}$.

[10]) Daß ich mich bei der Definition der Quasihauptideale auf ganze Ideale beschränkt habe, hat seinen Grund nur darin, daß in den Anwendungen von § 4 nur von ganzen Idealen die Rede ist. Im übrigen kann die Definition sofort auf gebrochene Ideale ausgedehnt werden.

[11]) Vgl.: Ein Hauptsatz über umkehrbare Ideale, Math. Zeitschrift **31** (1930).

eindeutig als Produkt endlich vieler paarweise teilerfremder Primideale darstellbar ist, sowie daß die Primideale von $\mathfrak{m}$ (außer $\mathfrak{m}$ selbst) keine echten Teiler besitzen, daß also das Restklassensystem von $\mathfrak{m}$ nach einem beliebigen Primideal stets ein Körper ist. $\mathfrak{m}$ hat also kurz gesagt arithmetrisch stets genau dieselbe Struktur wie der Ring $\mathfrak{o}$ aller ganzen Zahlen eines endlichen algebraischen Zahlkörpers. Wir können und wollen daher, soweit es uns zweckdienlich ist, alle die rein mit der Idealzerlegung zusammenhängenden Sätze, die von der Theorie der endlichen algebraischen Zahlkörper her bekannt sind, unmittelbar auf die allgemeinen Multiplikationsringe anwenden. Insbesondere können wir jedem Primideal $\mathfrak{p}$ von $\mathfrak{m}$ einen $\mathfrak{p}$-*adischen Ring* $\mathfrak{m}_\mathfrak{p}$ durch das folgende von den Henselschen „π-adischen Zahlringen" her bekannte Konstruktionsverfahren zuordnen [12]).

Elemente von $\mathfrak{m}_\mathfrak{p}$ seien die sämtlichen unendlichen Folgen $\{a_1, a_2, \ldots\}$ von Elementen aus $\mathfrak{m}$, die der „Verträglichkeitsbedingung hinsichtlich $\mathfrak{p}$": $a_i \equiv a_{i+1}\ (\mathfrak{p}^i)$ $(i = 1, 2, \ldots)$ genügen. Gleichheit, Addition, Multiplikation seien erklärt durch die Festsetzungen: $\{a_1, a_2, \ldots\} = \{b_1, b_2, \ldots\}$ d. u. n. d., wenn $a_i = b_i\ (\mathfrak{p}^i)$ $(i = 1, 2, \ldots)$; $\{a_1, a_2, \ldots\} \dot{+} \{b_1, b_2, \ldots\} = \{a_1 \dot{+} b_1, a_2 \dot{+} b_2, \ldots\}$. — Das Primideal $\bar{\mathfrak{p}}$, hinsichtlich dessen $\mathfrak{m}_\mathfrak{p}$ abgeschlossen ist, besteht aus allen und nur den Folgen, deren sämtliche Glieder durch $\mathfrak{p}$ teilbar sind. Die Folge $\{a_1, a_2, \ldots\}$ ist Basiselement von $\bar{\mathfrak{p}}^r$, wenn ihre Glieder von a_{r+1} ab genau durch die r-te Potenz von $\mathfrak{p}$ teilbar sind. Identifiziert man, was erlaubt ist und in Zukunft stets geschehen soll, die Folge $\{a, a, \ldots\}$ aus $\mathfrak{m}_\mathfrak{p}$ jeweils mit dem Element a aus $\mathfrak{m}$, so erscheint $\mathfrak{m}_\mathfrak{p}$ als Obermenge von $\mathfrak{m}$, *es wird der Bereich aller Ideale aus* $\mathfrak{m}$ *zum Bereich aller Potenzen von* $\mathfrak{p}$ *aus* $\mathfrak{m}_\mathfrak{p}$ *äquivalent*, und es gilt außerdem:

Hilfssatz 1. *Der Durchschnitt* $\mathfrak{m}'_\mathfrak{p}$ *von* $\mathfrak{m}_\mathfrak{p}$ *mit dem Quotientenkörper* $\mathfrak{k}$ *von* $\mathfrak{m}$ *besteht aus allen und nur den Elementen, die sich als Quotienten von Elementen aus* $\mathfrak{m}$ *mit durch* $\mathfrak{p}$ *unteilbarem Nenner darstellen lassen. — Jedes Element aus* $\mathfrak{m}_\mathfrak{p}$ *ist in* $\mathfrak{m}_\mathfrak{p}$ *einem Element aus* $\mathfrak{m}$ *äquivalent; jedes volle Restsystem von* $\mathfrak{m}$ *nach* $\mathfrak{p}^i$ *ist auch ein volles Restsystem von* $\mathfrak{m}_\mathfrak{p}$ *nach* $\bar{\mathfrak{p}}^i$ [13]).

§ 4. Potenzreihen mit Koeffizienten aus einem Multiplikationsring.

Es bedeute $\mathfrak{m}$ einen Multiplikationsring mit dem Quotientenkörper $\mathfrak{k}$, $\mathfrak{M}$ bzw. $\mathfrak{K}$ sei der Integritätsbereich aller Potenzreihen einer Variablen x mit Koeffizienten aus $\mathfrak{m}$ bzw. $\mathfrak{k}$. Ist a irgendein Element aus $\mathfrak{k}$, so können wir in Anbetracht der in § 3 über die Zerlegbarkeit der ganzen Ideale von $\mathfrak{m}$ gemachten Bemerkungen das gebrochene Ideal (a) von $\mathfrak{m}$ eindeutig als Produkt von positiven oder negativen Potenzen endlich vieler paarweise teilerfremder Primideale darstellen: $(a) = \mathfrak{p}_1^{r_1} \cdot \mathfrak{p}_2^{r_2} \cdots \mathfrak{p}_s^{r_s} \cdot \mathfrak{p}_{s+1}^{-r_{s+1}} \cdot \mathfrak{p}_{s+2}^{-r_{s+2}} \cdots \mathfrak{p}_{s+t}^{-r_{s+t}}$. Wir wollen $\mathfrak{p}_1^{r_1} \cdot \mathfrak{p}_2^{r_2} \cdots \mathfrak{p}_s^{r_s}$ als den Idealzähler, $\mathfrak{p}_{s+1}^{+r_{s+1}} \cdot \mathfrak{p}_{s+2}^{+r_{s+2}} \cdots \mathfrak{p}_{s+t}^{+r_{s+t}}$ als den Idealnenner von a bezeichnen. Dann gilt:

Hilfssatz 2. *Sind* P, Q, R *Potenzreihen in* x, *die der Gleichung* $P = Q \cdot R$ *genügen, und gehören* P *und* Q *zu* $\mathfrak{M}$, *so gehört* R *zu* $\mathfrak{K}$, *und es gehen in den Idealnennern der Koeffizienten von* R *nur solche Primideale auf, die auch im Anfangsglied von* Q *aufgehen.*

Die Richtigkeit von Hilfssatz 2 ergibt sich unmittelbar durch formale Berechnung von R aus P und Q.

Wir untersuchen jetzt die für die ganzen Ideale von $\mathfrak{M}$, insbesondere für die Quasihauptideale gültigen Zerlegungsgesetze. Dabei können und wollen wir uns auf die Betrachtung von solchen Idealen beschränken, die durch das Primideal (x) unteilbar sind.

---

[12]) Das Konstruktionsverfahren des Textes geht letzten Endes auf H. Prüfer zurück. Vgl. z. B. H. Prüfer, Eine neue Begründung der algebraischen Zahlentheorie, Math. Annalen **94** (1925), S. 198—243.

[13]) Der Beweis unsrer Behauptungen darf wohl unterdrückt werden, da er genau so geführt werden kann wie in dem bekannten Spezialfall der gewöhnlichen p-adischen oder π-adischen Zahlen.

Denn es läßt sich ja jedes Ideal aus $\mathfrak{M}$ eindeutig als Produkt einer Potenz von (x) mit einem durch (x) unteilbaren Ideal darstellen. — Ist $\mathfrak{A}$ ein beliebiges Ideal aus $\mathfrak{M}$, so bildet die Gesamtheit der Elemente aus $\mathfrak{m}$, die Anfangsglieder der Reihen von $\mathfrak{A}$ sind, ein Ideal $\mathfrak{a}$ *aus* $\mathfrak{m}$, das nach dem Vorbild von J. Schur [14]) als *Leitideal* von $\mathfrak{A}$ bezeichnet werden soll. Das Leitideal des Produktes ist offenbar das Produkt der Leitideale der einzelnen Faktoren, und es ist $\mathfrak{M}$ selbst das einzige Ideal mit dem Leitideal $\mathfrak{m}$. Aus diesen Bemerkungen ergibt sich sofort:

Hilfssatz 3. *Ist das Ideal* $\mathfrak{B}$ *aus* $\mathfrak{M}$ *Vielfaches des Quasihauptideals* $\mathfrak{A}$, *und besitzen* $\mathfrak{A}$ *und* $\mathfrak{B}$ *gleiche Leitideale, so ist* $\mathfrak{A} = \mathfrak{B}$.

In der Tat, als Quasihauptideal ist $\mathfrak{A}$ Faktor von $\mathfrak{B}$, $\mathfrak{A} \cdot \mathfrak{C} = \mathfrak{B}$ und wegen der Gleichheit der Leitideale von $\mathfrak{A}$ und $\mathfrak{B}$ muß $\mathfrak{C}$ das Leitideal $\mathfrak{m}$ besitzen und somit gleich $\mathfrak{M}$ sein. — Wir wenden uns jetzt zum Beweis des folgenden Fundamentalsatzes:

Satz 2. *In* $\mathfrak{M}$ *läßt sich jedes Quasihauptideal eindeutig als Produkt von Primidealen darstellen, die selbst Quasihauptideale sind* [15]).

Wir verstehen analog wie in § 3 unter $\mathfrak{m}_\mathfrak{p}$ den zu dem Primideal von $\mathfrak{m}$ gehörigen $\mathfrak{p}$-adischen Ring und bezeichnen mit $\mathfrak{M}_\mathfrak{p}$ den Integritätsbereich der Potenzreihen in x mit Koeffizienten aus $\mathfrak{m}_\mathfrak{p}$. Dann beweisen wir:

Hilfssatz 4. *Der Bereich derjenigen Quasihauptideale von* $\mathfrak{M}$, *deren Leitideale Potenzen des Primideals* $\mathfrak{p}$ *aus* $\mathfrak{m}$ *darstellen, ist zum Bereich der Hauptideale von* $\mathfrak{M}_\mathfrak{p}$ *äquivalent.*

Hilfssatz 5. *Ist* $\mathfrak{A}$ *ein beliebiges Quasihauptideal aus* $\mathfrak{M}$ *und ist* $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdot \mathfrak{p}_2^{r_2} \cdots \mathfrak{p}_s^{r_s}$ *die Zerlegung des Leitideals von* $\mathfrak{A}$ *in Potenzen teilerfremder Primideale, so besitzt* $\mathfrak{A}$ *eine eindeutig bestimmte Produktzerlegung* $\mathfrak{A} = \mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdots \mathfrak{A}_s$, *bei der* $\mathfrak{A}_i$ *gerade ein Quasihauptideal mit dem Leitideal* $\mathfrak{p}_i^{r_i}$ *darstellt.*

Aus Hilfssatz 4 und Hilfssatz 5 zusammen folgt sofort die Richtigkeit von Satz 2. Denn es läßt sich ja nach Satz 1 von § 2 in $\mathfrak{M}_\mathfrak{p}$ jedes Hauptideal eindeutig als Produkt von solchen Primidealen darstellen, die selbst Hauptideale sind. Den Beweis von Hilfssatz 4 und 5 wiederum stützen wir auf:

Hilfssatz 6. *Ist* $\mathfrak{A}_\mathfrak{p}$ *ein Hauptideal aus* $\mathfrak{M}_\mathfrak{p}$ *mit dem Leitideal* $\overline{\mathfrak{p}}^r$, *so ist das Verengungsideal von* $\mathfrak{A}_\mathfrak{p}$ *hinsichtlich* $\mathfrak{M}$ *ein Quasihauptideal mit dem Leitideal* $\mathfrak{p}^r$.

Hilfssatz 7. *Das Zurückleitungsideal eines Quasihauptideals* $\mathfrak{A}$ *von* $\mathfrak{M}$ *hinsichtlich* $\mathfrak{M}_\mathfrak{p}$ *ist selbst ein Quasihauptideal und zwar besitzt es als Leitideal die höchste Potenz von* $\mathfrak{p}$, *die im Leitideal von* $\mathfrak{A}$ *aufgeht.*

Wir wenden uns zunächst zum Beweise von Hilfssatz 6. Es sei $A_\mathfrak{p}$ ein Basiselement von $\mathfrak{A}_\mathfrak{p}$, a sei das Anfangsglied von $A_\mathfrak{p}$. Da jedes Element aus $\mathfrak{m}_\mathfrak{p}$ einem Element aus $\mathfrak{m}$ äquivalent ist, dürfen wir von vornherein a als Element von $\mathfrak{m}$ annehmen, und da $\overline{\mathfrak{p}}^r$ das Leitideal von $\mathfrak{A}_\mathfrak{p}$ sein sollte, muß dann für das Hauptideal (a) im $\mathfrak{m}$ eine Produktzerlegung $(a) = \mathfrak{p}^r \cdot \mathfrak{q}$ mit zu $\mathfrak{p}$ teilerfremdem $\mathfrak{q}$ gelten. Aus der Teilerfremdheit von $\mathfrak{q}$ und $\mathfrak{p}^r$ schließt man mühelos, daß in $\mathfrak{m}$ ein volles Restsystem $\mathfrak{r}^*$ von $\mathfrak{m}$ nach $\mathfrak{p}^r$ existieren muß, dessen sämtliche Elemente durch $\mathfrak{q}$ teilbar sind. Setzt man nun im Normierungshilfssatz $\mathfrak{J} = \mathfrak{M}_\mathfrak{p}$, $\mathfrak{p} = \overline{\mathfrak{p}}$, $a = a_0^* = a$, $e = 1$, $\mathfrak{r} = \mathfrak{r}^*$, so erkennt man, daß in $\mathfrak{M}$ eine Reihe A mit dem Anfangsglied a existieren muß, die in $\mathfrak{M}_\mathfrak{p}$ zu $A_\mathfrak{p}$ äquivalent also

[14]) Vgl. S. § 1, S. 37; K. § 1.

[15]) Bewiesen wird der Satz unserer Festsetzung gemäß nur für durch (x) unteilbare Quasihauptideale. Seine Allgemeingültigkeit ist dann trivial. Der Satz 2 des Textes ist vollständig gleichwertig dem Satz von S. § 6 (S. 106). Um das einzusehen, hat man sich nur von der Richtigkeit der folgenden, leicht beweisbaren Tatsache zu überzeugen: Ein durch (x) unteilbares Ideal $\mathfrak{A}$ aus $\mathfrak{M}$ ist dann und nur dann Quasihauptideal, wenn $\mathfrak{A}$ im Sinne von S. § 2 (S. 98) den Index 0 hat, d. h. wenn die Ideale $\mathfrak{A}, \mathfrak{A} : (x), \mathfrak{A} : (x^2), \mathfrak{A} : (x^3), \ldots$ sämtlich das gleiche Leitideal besitzen.

Basiselement von $\mathfrak{A}_\mathfrak{p}$ ist, und deren Koeffizienten sämtlich durch $\mathfrak{q}$ teilbar sind. Es sei jetzt e ein (sicher vorhandenes) Element aus $\mathfrak{k}$ mit dem Idealnenner $\mathfrak{q}$ und mit einem zu $\mathfrak{p}$ teilerfremden Idealzähler $\mathfrak{q}'$, $\mathfrak{c}$ sei das (gebrochene) Ideal von $\mathfrak{m}$ mit der Basis $(1, c)$. Dann ist in $\mathfrak{m}$ das Hauptideal $(c \cdot a)$ gleich $\mathfrak{p}^r \cdot \mathfrak{q}'$, $B = c \cdot A$ ist eine zu A in $\mathfrak{M}_\mathfrak{p}$ äquivalente Reihe aus $\mathfrak{M}$ mit dem Anfangsglied $c \cdot a$, und es stellt $(A, c \cdot A) = \mathfrak{c} \cdot (A)$ ein Quasihauptideal aus $\mathfrak{M}$ mit dem Leitideal $\mathfrak{p}^r$ dar. Wir behaupten nun, daß $\mathfrak{c} \cdot (A)$ mit dem Verengungsideal $\mathfrak{A}$ von $\mathfrak{A}_\mathfrak{p}$ hinsichtlich $\mathfrak{M}$ identisch ist.

In der Tat, zunächst ist $\mathfrak{A}$ sicher Obermenge von $\mathfrak{c} \cdot (A)$. Es sei ferner C eine beliebige Reihe aus $\mathfrak{A}$; dann muß C in $\mathfrak{M}_\mathfrak{p}$ sowohl durch A als auch durch $c \cdot A$ teilbar sein, es gelten also zwei Gleichungen $C = A \cdot Q = c \cdot A \cdot (c^{-1} \cdot Q)$ mit zu $\mathfrak{M}_\mathfrak{p}$ gehörigem Q und $c^{-1} \cdot Q$, und die Anwendung von Hilfssatz 1 und 2 zeigt, daß Q bzw. $c^{-1} \cdot Q$ Reihen aus $\mathfrak{R}$ sein müssen, bei denen in den Idealnennern der Koeffizienten nur solche Primideale aufgehen, die Teiler von $\mathfrak{q}$ bzw. $\mathfrak{q}'$ sind. Daraus folgt sofort, daß die Produkte von Q bzw. $Q \cdot c^{-1}$ mit den Elementen von $\mathfrak{q}$ bzw. $\mathfrak{q}'$ sämtlich zu $\mathfrak{M}$ gehören müssen. Es ist also in $\mathfrak{M}$ das Quasihauptideal $\mathfrak{q} \cdot (C)$ durch (A), das Quasihauptideal $\mathfrak{q}' \cdot (C)$ durch (B) teilbar, und daraus ergibt sich wegen der Teilerfremdheit von $\mathfrak{q}$ und $\mathfrak{q}'$ die Teilbarkeit von (C) durch $\mathfrak{c} \cdot (A) = (A, B)$. Es gehört also jede Reihe C aus $\mathfrak{A}$ zu $\mathfrak{c} \cdot (A)$, die Identität von $\mathfrak{A}$ und $\mathfrak{c} \cdot (A)$ und damit die Richtigkeit von Hilfssatz 6 ist voll bewiesen. Um von Hilfssatz 6 auf Hilfssatz 7 schließen zu können, braucht man nur zu zeigen:

Ist $\mathfrak{A}$ ein beliebiges Quasihauptideal aus $\mathfrak{M}$, so stellt das Erweiterungsideal $\mathfrak{A} \cdot \mathfrak{M}_\mathfrak{p}$ von $\mathfrak{A}$ hinsichtlich $\mathfrak{M}_\mathfrak{p}$ ein Hauptideal dar, dessen Leitideal genau gleich $\overline{\mathfrak{p}}^r$ ist, falls $\mathfrak{p}^r$ die höchste Potenz von $\mathfrak{p}$ bedeutet, die im Leitideal von $\mathfrak{A}$ aufgeht. Es sei $\mathfrak{A} = \mathfrak{c} \cdot (A)$; dann muß es in $\mathfrak{A}$ eine Reihe $A^* = c \cdot A$ (c aus $\mathfrak{k}$) geben, deren Anfangsglied genau durch die r-te Potenz von $\mathfrak{p}$ teilbar ist, und man sieht sofort, daß jede Reihe aus A in der Form $A^* \cdot d$ darstellbar sein muß, wobei d ein Element aus $\mathfrak{k}$ mit durch $\mathfrak{p}$ unteilbarem Idealnenner, also ein Element aus $\mathfrak{M}_\mathfrak{p}$ bedeutet. Daraus folgt aber, daß $\mathfrak{A} \cdot \mathfrak{M}_\mathfrak{p}$ in $\mathfrak{M}_\mathfrak{p}$ die eingliedrige Basis (A^*) besitzt, und da das Anfangsglied von A^* genau durch $\mathfrak{p}^r$ teilbar ist, muß $\overline{\mathfrak{p}}^r$ das Leitideal von $A \cdot \mathfrak{M}_\mathfrak{p}$ sein.

Aus den nunmehr voll bewiesenen Hilfssätzen 6 und 7 sowie aus Hilfssatz 3 ergibt sich:

Ein Hauptideal aus $\mathfrak{M}_\mathfrak{p}$ ist stets mit seinem Zurückleitungsideal hinsichtlich $\mathfrak{M}$ identisch. Ein Quasihauptideal aus $\mathfrak{M}$ ist dann und nur dann mit seinem Zurückleitungsideal hinsichtlich $\mathfrak{M}_\mathfrak{p}$ identisch, wenn sein Leitideal eine Potenz von $\mathfrak{p}$ darstellt. Es muß daher für jedes $\mathfrak{p}$ der Bereich der Hauptideale von $\mathfrak{M}_\mathfrak{p}$ zum Bereich derjenigen Quasihauptideale von $\mathfrak{M}$, die Potenzen von $\mathfrak{p}$ als Leitideale besitzen, äquivalent sein, d. h. es muß Hilfssatz 4 allgemein gelten.

Zum vollen Beweis von Satz 2 haben wir somit nur noch die Richtigkeit von Hilfssatz 5 zu zeigen. Es sei also $\mathfrak{A}$ ein beliebiges Quasihauptideal aus $\mathfrak{M}$, $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdot \mathfrak{p}_2^{r_2} \cdots \mathfrak{p}_s^{r_s}$ sei die Zerlegung seines Leitideals $\mathfrak{a}$ in Potenzen teilerfremder Primideale; ferner bedeute $\mathfrak{A}^i$ für jedes i das Zürückleitungsideal von $\mathfrak{A}$ hinsichtlich $\mathfrak{M}_{\mathfrak{p}_i}$. Dann ist $\mathfrak{A}_i$ ein Quasihauptideal mit dem Leitideal $\mathfrak{p}_i^{r_i}$, und es müssen für $i \neq k$ die Ideale $\mathfrak{A}_i$ und $\mathfrak{A}_k$ wegen der Teilerfremdheit ihrer Leitideale $\mathfrak{p}_i^{r_i}$ und $\mathfrak{p}_k^{r_k}$ stets teilerfremd sein. Daraus folgt aber nach bekannten Sätzen, daß $\mathfrak{A}$ nicht nur durch jedes einzelne $\mathfrak{A}_i$, sondern auch durch das Produkt $\mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdots \mathfrak{A}_s$ teilbar ist, und da $\mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdots \mathfrak{A}_s$ ein Quasihauptideal mit demselben Leitideal wie $\mathfrak{A}$ darstellt, muß nach Hilfssatz 3 die Gleichung $\mathfrak{A} = \mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdots \mathfrak{A}_s$ gelten. Damit ist gezeigt, daß mindestens eine Produktzerlegung der in Hilfssatz 5 geforderten Art existiert, und die Eindeutigkeit der gefundenen Zerlegung ergibt sich unmittelbar aus der Teilerfremdheit der Faktoren.

Es ist also auch Hilfssatz 5 als richtig nachgewiesen, der Beweis von Satz 2 ist restlos erbracht. Es wäre auch möglich gewesen, den Satz 2 direkt, ohne Benutzung der Ringe $\mathfrak{M}_\mathfrak{p}$ und des Hilfssatzes 4 abzuleiten. Unsere Methode hat indessen den großen Vorzug, daß sie uns eine genauere Charakterisierung derjenigen Quasihauptideale aus $\mathfrak{M}$ ermöglicht, die Primideale sind. Wir erhalten:

Satz 3. *Soll das Quasihauptideal $\mathfrak{A}$ aus $\mathfrak{M}$ Primideal sein, und ist nicht gerade $\mathfrak{A} = (x)^r$, so muß jedenfalls das Leitideal von $\mathfrak{A}$ eine Primidealpotenz in $\mathfrak{m}$ darstellen. Ist ferner das Leitideal von $\mathfrak{A}$ gleich der r-ten Potenz des Primideals $\mathfrak{p}$, ist $\mathfrak{A} \neq \mathfrak{p} \cdot \mathfrak{M}$, und bedeutet A eine Reihe aus $\mathfrak{A}$, deren Anfangsglied durch $\mathfrak{p}^r$, aber nicht durch $\mathfrak{p}^{r+1}$ teilbar ist, so stellt $\mathfrak{A}$ dann und nur dann ein Primideal in $\mathfrak{M}$ dar, wenn A in $\mathfrak{M}_\mathfrak{p}$ eine irreduzible Weierstraßsche Normalform besitzt, also daselbst einem im Koeffizientenring $\mathfrak{M}_\mathfrak{p}$ irreduzibeln Polynom äquivalent ist.*

Der Beweis von Seite 3 folgt unmittelbar aus den beim Beweise von Satz 2 benutzten Schlüssen, insbesondere aus Hilfssatz 4 und 5, sowie aus Satz 1 von § 2. Satz 3, der die Frage nach dem Primidealcharakter eines Quasihauptideals aus $\mathfrak{M}$ auf die Untersuchung der Irreduzibilität eines Polynoms zurückführt, ist vor allem deshalb von Wichtigkeit, weil er uns unter Umständen gestattet, mit endlich viel Schritten darüber zu entscheiden, ob ein vorgelegtes Quasihauptideal aus $\mathfrak{M}$ Primideal ist oder nicht.

Es sei z. B. $\mathfrak{m}$ der Ring aller ganzen Zahlen eines endlichen algebraischen Zahlkörpers. Dann sind die $\mathfrak{m}_\mathfrak{p}$ die zu den einzelnen Primidealen von $\mathfrak{m}$ gehörigen Henselschen π-adischen Zahlringe und man kann nach Hensel [16]) durch eine endliche Anzahl von Versuchen feststellen, ob ein Polynom mit Koeffizienten aus einem π-adischen Zahlring irreduzibel ist oder nicht. Ist daher in diesem Falle irgendein Quasihauptideal $\mathfrak{A}$ aus $\mathfrak{M}$ vorgelegt, und kennen wir zu irgendeiner Reihe A aus $\mathfrak{A}$ mit genau durch $\mathfrak{p}^r$ teilbarem Anfangsglied die Weierstraßsche Normalform, so können wir mit endlich viel Schritten über den Primidealcharakter von $\mathfrak{A}$ entscheiden. Ist dagegen zu keinem A die Weierstraßsche Normalform A^* von vornherein gegeben, so muß man versuchen, zu einem festen A das zugehörige A^* irgendwie zu berechnen. Das wird allerdings im allgemeinen nicht mit endlich viel Schritten zu machen sein; denn wie sehr man auch die Rechnung vereinfacht, stets wird man letzten Endes so vorgehen müssen, daß man die gesuchte Normalform A^* als Potenzreihe in einem Primelement π aus $\mathfrak{m}_\mathfrak{p}$ ansetzt und die unendlich vielen Koeffizienten dieser Reihe irgendwie sukzessive ermittelt. Indes genügt es nach den Henselschen Untersuchungen in vielen Fällen zur Entscheidung über die Polynomirreduzibilität von A^* im Koeffizientenring $\mathfrak{m}_\mathfrak{p}$, wenn man die Koeffizienten von A^* nicht genau, sondern nur ihrem Restcharakter nach einer hinreichend hohen Potenz von $\bar{\mathfrak{p}}$ nach kennt; und in allen diesen Fällen wird man wieder mit endlich viel Schritten entscheiden können, ob das vorgelegte Quasihauptideal $\mathfrak{A}$ Primideal ist oder nicht. — Unter diesem Gesichtspunkt erscheint das in Satz 3 niedergelegte Ergebnis als der geeignetste Ausgangspunkt zur Aufstellung von Primidealkriterien für die Quasihauptideale von $\mathfrak{M}$ nach dem Vorbild der Irreduzibilitätskriterien für Polynome mit ganzen rationalen oder ganzen algebraischen Koeffizienten. *Wir verzichten darauf, die aufgestellte Behauptung durch Beispiele zu erhärten, obwohl das an und für sich leicht möglich wäre.*

§ 5. Konvergente Reihen.

Hat man es bei dem Multiplikationsring $\mathfrak{m}$ mit dem Ring aller ganzen algebraischen Zahlen eines endlichen Zahlkörpers oder allgemeiner mit einem beliebigen Unterring des Körpers aller komplexen Zahlen zu tun, so liegt die Frage auf der Hand, inwieweit sich die Ergebnisse von § 4 vom Ring $\mathfrak{M}$ aller *formalen* Potenzreihen in x mit

[16]) Vgl. z. B. K. Hensel, Lehrbuch der Zahlentheorie.

Koeffizienten aus $\mathfrak{m}$ auf den Ring $\mathfrak{M}^*$ aller *konvergenten* Potenzreihen in x mit Koeffizienten aus $\mathfrak{m}$ übertragen lassen. Die Antwort lautet einfach: *Die ganze Theorie von* § 4 *gilt ebenso wie für* $\mathfrak{M}$ *auch für* $\mathfrak{M}^*$, denn wir können feststellen:

Satz 4. *Ist* $\mathfrak{m}$ *ein ganzzahliger Unterring des Körpers der komplexen Zahlen, und ist* $\mathfrak{M}$ *bzw.* $\mathfrak{M}^*$ *der Integritätsbereich aller formalen bzw. konvergenten Potenzreihen in* x *mit Koeffizienten aus* $\mathfrak{m}$, *so sind die zu* $\mathfrak{M}$ *und* $\mathfrak{M}^*$ *gehörigen Idealbereiche äquivalent.*

Den Satz 4 habe ich bereits in K. für den Spezialfall bewiesen[17]), daß $\mathfrak{m} = \mathfrak{o}$ den Ring aller ganzen Zahlen eines endlichen algebraischen Zahlkörpers darstellt, und zwar benutzte ich dabei, wie eine Analyse des Beweises zeigt, nur die folgende besondere Eigenschaft von $\mathfrak{o}$: Zu jedem Ideal $\mathfrak{a}$ von $\mathfrak{o}$ gibt es ein volles Restsystem $\mathfrak{r}$ von $\mathfrak{o}$ nach $\mathfrak{a}$, derart, daß jede Potenzreihe, deren Koeffizienten fast alle zu $\mathfrak{o}$ gehören, konvergiert. Diese Eigenschaft kommt aber in Wirklichkeit nicht nur den Ringen $\mathfrak{o}$, sondern jedem beliebigen Unterring des Körpers der komplexen Zahlen zu, denn es gilt:

Hilfssatz 8. *Ist* $\mathfrak{m}$ *ein beliebiger Unterring des Körpers der komplexen Zahlen, und bedeutet* $\mathfrak{a}$ *ein beliebiges Ideal aus* $\mathfrak{m}$, *so gibt es ein stets beschränktes volles Restsystem von* $\mathfrak{m}$ *nach* $\mathfrak{a}$.

Beim Beweis wollen wir, um gleich den verhältnismäßig schwierigeren Fall zu behandeln, voraussetzen, daß $\mathfrak{m}$ nicht ausschließlich aus reellen Zahlen besteht. Es sei $a \neq 0$ eine beliebige Zahl aus $\mathfrak{a}$, $c \neq 0$ eine beliebige nicht reelle Zahl aus $\mathfrak{m}$. Dann bildet die Gesamtheit der Zahlen $n \cdot a$, $n \cdot c \cdot a$ $(n = 0, \pm 1, \pm 2, \ldots)$ die Gesamtheit der Ecken eines Parallelogrammnetzes in der komplexen Zahlenebene, und aus der Tatsache, daß alle Zahlen $n \cdot a$, $n \cdot c \cdot a$ in $\mathfrak{a}$ enthalten sind, folgt sofort, daß man ein volles Restsystem $\mathfrak{r}$ von $\mathfrak{m}$ nach $\mathfrak{a}$ so wählen kann, daß alle Elemente von $\mathfrak{r}$ ganz im Innern oder auf dem Rande eines festen Parallelogramms des genannten Netzes liegen.

Damit ist Hilfssatz 8 bewiesen, und da jede Potenzreihe mit beschränkten Koeffizienten konvergiert, ergibt sich aus dem Normierungshilfssatz, daß jede Reihe aus $\mathfrak{M}$ einer Reihe aus $\mathfrak{M}^*$ äquivalent ist, und daraus folgt sofort weiter, daß jedes Ideal aus $\mathfrak{M}$ mit seinem Zurückleitungsideal hinsichtlich $\mathfrak{M}^*$ identisch sein muß.

Um umgekehrt nachzuweisen, daß jedes Ideal aus $\mathfrak{M}^*$ mit seinem Zurückleitungsideal hinsichtlich $\mathfrak{M}$ identisch ist, braucht man nur zu zeigen: Gilt eine Gleichung $A_1^* \cdot B_1 + A_2^* \cdot B_2 + \cdots + A_s^* \cdot B_s = A^*$, wobei $A_1^*, A_2^*, \ldots, A_s^*, A^*$ zu $M^*, B_1, B_2, \ldots, B_s$ zu M gehören, so gilt auch eine Gleichung $A_1^* \cdot B_1^* + A_2^* \cdot B_2^* + \cdots + A_s^* \cdot B_s^* = A^*$ mit zu M^* gehörigen B_i^*. — Es sei $A^* = c_r x^r + c_{r+1} x^{r+1} + \cdots$, $c_r \neq 0$, $\mathfrak{a} = (c_r)$, $\mathfrak{r}$ bedeute ein beschränktes volles Restsystem von $\mathfrak{m}$ nach $\mathfrak{a}$. Dann zeigt man leicht mit den vom Normierungshilfssatz her bekannten Schlüssen[18]), daß in $\mathfrak{M}$ die Reihen $C_2^*, C_3^*, \ldots, C_s^*$ so bestimmt werden können, daß in $B_i^* = B_i - C_i^* \cdot A_1^*$ $(i = 2, 3, \ldots, s)$ die Koeffizienten von $x^r, x^{r+1}, \ldots$ sämtlich zu $\mathfrak{r}$ gehören. Setzt man nun $B_1^* = B_1 + \sum_{i=2}^{s} C_i^* \cdot A_i^*$, so wird $A^* = \sum_{i=1}^{s} A_i^* \cdot B_i^*$, und es konvergiert neben $B_2^*, B_3^*, \ldots, B_s^*$ auch B_1^* als Quotient der konvergenten Reihen $A^* - \sum_{i=2}^{s} A_i^* \cdot B_i^*$ und A_1^*.

Es ist also auch jedes Ideal aus $\mathfrak{M}^*$ mit seinem Zurückleitungsideal hinsichtlich $\mathfrak{M}$ identisch. Satz 4 ist in vollem Umfange bewiesen.

[17]) K. Satz 9. Der Beweis ist allerdings an der genannten Stelle kaum skizziert.

[18]) Vgl. analoge Schlüsse bei S. (§ 2, S. 99), die hier auch den Ausgangspunkt zur Formulierung des Normierungshilfssatzes bildeten.

Eingegangen 18. März 1930.

Eine Bemerkung über rationalzahlige Potenzreihen.

Von *Wolfgang Krull* in Erlangen.

Die Theorie der ganzzahligen Polynome in zwei Variabeln x und y (oder auch in endlich viel Variabeln $x_1, x_2, \ldots, x_n$) kann bekanntlich ohne Schwierigkeit auf die Theorie der rationalzahligen Polynome zurückgeführt werden, und zwar im wesentlichen auf Grund der Tatsache, daß jedes rationalzahlige Polynom durch Multiplikation mit einer ganzen Zahl in ein ganzzahliges verwandelt werden kann[1]). Im folgenden soll nun durch ein Beispiel gezeigt werden, daß die Verhältnisse sicher bei weitem nicht so einfach liegen, wenn es sich nicht um Polynome, sondern um Potenzreihen handelt.

Wir verstehen unter einer Potenzreihe eine formale oder konvergente, ausschließlich Potenzprodukte mit nichtnegativen Exponenten enthaltende Reihe in x und y mit rationalen oder ganzen rationalen Koeffizienten. Die Reihen seien nach Formen steigender Dimension geordnet: $Q(x, y) = \varphi_m + \varphi_{m+1} + \varphi_{m+2} + \cdots$ (φ_i homogene Form i-ten Grades in x und y, $\varphi_m \neq 0$), so daß also die Multiplikationsregel lautet: $Q(x, y) \cdot R(x, y) = (\varphi_m + \varphi_{m+1} + \cdots) \cdot (\psi_n + \psi_{n+1} + \cdots) = \varphi_m \cdot \psi_n + (\varphi_m \cdot \psi_{n+1} + \varphi_{m+1} \cdot \psi_n) + \cdots$.
Wir behaupten nun:

Satz. *Es sei p irgendeine Primzahl. Dann ist das Produkt $Q(x,y) \cdot Q^*(x,y) = R(x,y)$ niemals ganzzahlig, falls $Q(x, y)$ eine ganz beliebige von 0 verschiedene, $Q^*(x, y)$ dagegen die folgende spezielle Potenzreihe bedeutet:*

$$(1) \qquad Q^*(x, y) = y + \sum_{d=1!, 2!, 3!, \cdots} p^{-d!}\, x^{d+1} = y + \sum_{r=1, 2, 3, \cdots} \pi_r x^{r+1}.$$

Beweis indirekt! Wir nehmen an, es sei $R(x, y)$ ganzzahlig und folgern daraus, daß in $Q(x, y)$ ein Potenzprodukt mit negativem y-Exponenten auftreten muß, was unserer Definition der Potenzreihe widerspricht.

Es sei nach Formen steigender Dimension entwickelt $Q(x, y) = \chi_m + \chi_{m+1} + \cdots$; $R(x, y) = \psi_m + \psi_{m+1} + \cdots$. Dann zeigen wir zunächst die Richtigkeit der folgenden „ersten Hilfsbehauptung“:

Für $M = N!$, $L = (N-1)!$, $0 \leqq i < M - L$ ($N \geqq 1$, $0! = 0$) sind die Koeffizientennenner von χ_{m+L+i} höchstens durch $p^{(i+1)\cdot L!}$ teilbar, während die Koeffizienten von χ_{m+M} höchstens die $M!$-te Potenz von p im Nenner stehen haben.

Für $N = 1, 2$ erschließt man die Gültigkeit der ersten Hilfsbehauptung unmittelbar aus der Ganzzahligkeit von

$$\psi_{m+1} = y\chi_m,\ \psi_{m+2} = y\chi_{m+1} + p^{-1}x^2\chi_m,\ \psi_{m+3} = y\chi_{m+2} + p^{-1}x^2\chi_{m+1} + p^{-2}x^3\chi_m.$$

Nehmen wir ferner an, es sei bei festem $N - 1 \geqq 2$ die erste Hilfsbehauptung für jedes $M = J!$, bei dem $J \leqq N - 1$, bereits bewiesen, so ergibt sich die Richtigkeit der

[1]) Vgl. die ausführlichen Betrachtungen am Schlusse der Note.

ersten Hilfsbehauptung für $M = N!$ mühelos aus der Ganzzahligkeit der Formen $\psi_{m+L+2}, \psi_{m+L+3}, \cdots, \psi_{m+M+1}$, die angesichts der Definition der Koeffizienten π_i die folgende Gestalt annehmen:

$$
\begin{aligned}
\psi_{m+L+2} &= y\chi_{m+L+1} + p^{-1}x^2\chi_{m+L} + \cdots + p^{-L!}x^{L+1}\chi_{m+1} \\
\psi_{m+L+3} &= y\chi_{m+L+2} + p^{-1}x^2\chi_{m+L+1} + \cdots + p^{-L!}x^{L+1}\chi_{m+2} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\psi_{m+M} &= y\chi_{m+M-1} + p^{-1}x^2\chi_{m+M-2} + \cdots + p^{-L!}x^{L+1}\chi_{m+M-(L+1)} \\
\psi_{m+M+1} &= y\chi_{m+M} + p^{-1}x^2\chi_{m+M-1} + \cdots + p^{-L!}x^{L+1}\chi_{m+M-L} + p^{-M!}x^{M+1}\chi_m .
\end{aligned}
\tag{2}
$$

Man hat nur zu beachten, daß wegen der Induktionsvoraussetzung und der für $J < N-1$ gültigen Ungleichung $L! = ((N-1)!)! > (N-J)\cdot(J!)!$ die Koeffizientennenner von $\chi_{m+1}, \chi_{m+2}, \cdots, \chi_{m+L}$ sämtlich höchstens durch $p^{L!}$ teilbar sind.

Es sei jetzt R der Exponent der höchsten Potenz von p, die in sämtlichen Koeffizienten von χ_m aufgeht, und es sei $N \geqq 2$ so groß gewählt, daß für $N! = M$, $(N-1)! = L$ die folgenden Ungleichungen gelten:

(3 a) $\quad (N+1)! - M > m\,M;$ $\qquad$ (3 b) $\quad M! - R > (M+1)\cdot L!\,.$

Dann ist jedenfalls $\pi_M = p^{-M!}$, während wegen (3 a) $\pi_{M+1} = \pi_{M+2} = \cdots = \pi_{(m+1)\cdot M} = 0$ wird. Diese letztere Tatsache ermöglicht aber den Beweis der folgenden „zweiten Hilfsbehauptung“:

Für $i = 1, 2, \ldots, m+1$ muß in der Form χ_{m+iM} ein Potenzprodukt $x^{m+iM-s_i}y^{s_i}$ auftreten, bei dem der Exponent s_i höchstens gleich $m-i$ ist, und dessen Koeffizient einen durch $p^{i(M!-R)}$ teilbaren Nenner besitzt, also sicher von 0 verschieden ist.

Aus der zweiten Hilfsbehauptung folgt für $i = m+1$ bereits der gesuchte Widerspruch. Denn nach unserer Definition der Potenzreihen kann ja in keiner der Formen χ_{m+K} ein Potenzprodukt vorkommen, bei dem der Exponent von y negativ ist. Um nun zuerst die zweite Hilfsbehauptung für χ_{m+M} zu beweisen, brauchen wir angesichts der Ungleichung (3 b) in der letzten Gleichung von (2) nur zu beachten, daß die sämtlichen in $p^{-M!}x^{M+1}\chi_m$ wirklich vorkommenden Potenzprodukte alle Koeffizienten mit durch $p^{M!-R}$ teilbarem Nenner besitzen und daß diese Potenzprodukte sicher durch y^{m+1} unteilbar sind.

Um weiter von χ_{m+M} auf χ_{m+2M} zu schließen, bilden wir:

$$
\begin{aligned}
\psi_{m+M+2} &= y\chi_{m+M+1} + p^{-1}x^2\chi_{m+M} + \cdots + p^{-L!}x^{L+1}\chi_{m+M-L+1} + p^{-M!}x^{M+1}\chi_{m+1} \\
\psi_{m+M+3} &= y\chi_{m+M+2} + p^{-1}x^2\chi_{m+M+1} + \cdots + p^{-L!}x^{L+1}\chi_{m+M-L+2} + p^{-M!}x^{M+1}\chi_{m+2} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\psi_{m+2M} &= y\chi_{m+2M-1} + p^{-1}x^2\chi_{m+2M-2} + \cdots + p^{-L!}x^{L+1}\chi_{m+2M-L-1} + p^{-M!}x^{M+1}\chi_{m+M-1} \\
\psi_{m+2M+1} &= y\chi_{m+2M} + p^{-1}x^2\chi_{m+2M-1} + \cdots + p^{-L!}x^{L+1}\chi_{m+2M-L} + p^{-M!}x^{M+1}\chi_{m+M} .
\end{aligned}
\tag{4}
$$

Beachten wir nun die erste Hilfsbehauptung in der abgeschwächten Form, daß für $J < M$ die Koeffizientennenner von χ_{m+J} jedenfalls höchstens durch $p^{J\cdot L!}$ teilbar sind, so kann man aus den ersten $M-1$ Gleichungen von (4) der Reihe nach ohne Schwierigkeit ablesen, daß für $\varkappa = 1, 2, \ldots, M-1$ die Koeffizientennenner von $\chi_{m+M+\varkappa}$ jedenfalls höchstens die $(M! + \varkappa\cdot L!)$-te Potenz von p enthalten. Des ferneren muß wegen der für χ_{m+M} bereits bewiesenen Hilfsbehauptung in $p^{-M!}x^{M+1}\chi_{m+M}$ mindestens ein höchstens durch y^{m-1} teilbares Potenzprodukt vorkommen, dessen Koeffizient einen durch $p^{2\cdot M!-R}$ teilbaren Nenner besitzt. Daraus folgt aber mit Hilfe der letzten Gleichung von (2) und der Ungleichnug (3 b), daß die zweite Hilfsbehauptung auch für χ_{m+2M} richtig sein muß. Außerdem ergibt sich — gewissermaßen als Verschärfung der ersten Hilfsbehauptung —

aus dem Umstand, daß $p^{M!}\chi_{m+M}$ und somit auch $p^{2\cdot M!}(p^{-M!}x^{M+1}\chi_{m+M})$ ganzzahlig ist, daß die sämtlichen Koeffizientennenner von χ_{m+2M} höchstens durch $p^{2\cdot M!}$ teilbar sein können. Auf Grund dieser Feststellungen kann man aber genau so von χ_{m+2M} auf χ_{m+3M} schließen, wie wir eben von χ_{m+M} auf χ_{m+2M} geschlossen haben usw. Der Schluß von χ_{m+iM} auf $\chi_{m+(i+1)M}$ würde erst dann versagen, wenn unter den Koeffizienten $\pi_{M+1}, \pi_{M+2}, \cdots, \pi_{(i+1)M}$ ein von 0 verschiedener vorkäme. Da das wegen der Ungleichung (3 a) für $i \leqq m$ nicht der Fall ist, können wir die zweite Hilfsbehauptung der Reihe nach für $\chi_{m+3M}, \chi_{m+4M}, \cdots, \chi_{m+(m+1)M}$ beweisen, und so tatsächlich den gewünschten Widerspruch erzwingen.

Es soll nunmehr kurz auseinandergesetzt werden, was für arithmetische Folgerungen aus der Existenz und der Grundeigenschaft der Reihe $Q^*(x, y)$ gezogen werden können. Es bedeute $\mathfrak{A}_g$ bzw. $\mathfrak{A}_r$ den Ring der ganz- bzw. rationalzahligen Polynome, $\mathfrak{B}_g$ bzw. $\mathfrak{B}_r$ den Ring der ganz- bzw. rationalzahligen formalen Potenzreihen in x und y. Dann gilt zunächst für $\mathfrak{A}_g$ und $\mathfrak{B}_g$ der Satz, daß alle diejenigen Elemente aus $\mathfrak{A}_g$ bzw. $\mathfrak{B}_g$, die in $\mathfrak{A}_r$ bzw. $\mathfrak{B}_r$ zu Einheiten werden, (d. h. die von 0 verschiedenen Konstanten bzw. die Potenzreihen $E(x, y) = \varphi_0 + \varphi_1 + \cdots$ mit $\varphi_0 \neq 0$), in $\mathfrak{A}_g$ bzw. $\mathfrak{A}_r$ eindeutig in Primfaktoren zerlegt werden können [2]). Nennen wir ferner ein Element A bzw. B aus $\mathfrak{A}_g$ bzw. $\mathfrak{B}_g$ „primitiv", wenn jeder in $\mathfrak{A}_g$ bzw. $\mathfrak{B}_g$ auftretende Teiler von A bzw. B, der in $\mathfrak{A}_r$ bzw. $\mathfrak{B}_r$ Einheit wird, bereits in $\mathfrak{A}_g$ bzw. $\mathfrak{B}_g$ Einheit ist, so folgt aus der bereits hervorgehobenen Eigenschaft von $\mathfrak{A}_g$ bzw. $\mathfrak{B}_g$ weiter:

Jedes Element Q_a bzw. Q_b aus $\mathfrak{A}_g$ bzw. $\mathfrak{B}_g$ besitzt eine eindeutig bestimmte Produktzerlegung $Q_a = E_a P_a$ bzw. $Q_b = E_b P_b$, bei der P_a bzw. P_b primitiv ist, während E_a bzw. E_b in $\mathfrak{A}_r$ bzw. $\mathfrak{B}_r$ zur Einheit wird.

Bis hierher kann man also die Theorie von $\mathfrak{A}_g$ bzw. $\mathfrak{B}_g$ im wesentlichen in gleicher Weise entwickeln, jetzt aber beginnt der entscheidende Unterschied. Über den Zusammenhang zwischen $\mathfrak{A}_g$ und $\mathfrak{A}_r$ gilt der Satz: Sind A_1 und A_2 primitive Elemente aus $\mathfrak{A}_g$, und ist A_1 in $\mathfrak{A}_g$ kein Teiler von A_2, so ist A_1 auch in $\mathfrak{A}_r$ kein Teiler von A_2; jedes Element aus $\mathfrak{A}_r$ kann durch Multiplikation mit einer Einheit in ein primitives Element aus $\mathfrak{A}_g$ verwandelt werden, es ist „einem primitiven Element aus $\mathfrak{A}_g$ äquivalent". Aus diesen Sätzen folgt, daß die Hauptideale aus $\mathfrak{A}_g$ mit primitiver Basis eindeutig umkehrbar den sämtlichen Hauptidealen von $\mathfrak{A}_r$ entsprechen, und dieser Umstand in Verbindung mit den früher festgestellten Tatsachen macht es möglich, aus der eindeutigen Zerlegbarkeit der Elemente von $\mathfrak{A}_r$ in Primfaktoren auf die entsprechende Zerlegbarkeit der Elemente von $\mathfrak{A}_g$ zu schließen [3]).

Da nun in $\mathfrak{B}_r$ der gleiche Zerlegungssatz gilt wie in $\mathfrak{A}_r$ [4]), könnte man auch von den Elementen von $\mathfrak{B}_g$ die eindeutige Zerlegbarkeit in Primfaktoren behaupten —, wenn der Zusammenhang zwischen $\mathfrak{B}_g$ und $\mathfrak{B}_r$ ebenso durchsichtig wäre wie der zwischen $\mathfrak{A}_g$ und $\mathfrak{A}_r$. Daß das aber sicher nicht der Fall ist, zeigt z. B. gerade unsere oben untersuchte Reihe $Q^*(x, y)$. *Denn Q^* teilt ja (in $\mathfrak{B}_r$) überhaupt keine von 0 verschiedene Reihe von $\mathfrak{B}_g$, ist also auch sicher keiner Reihe von $\mathfrak{B}_g$ äquivalent.*

---

[2]) Für $\mathfrak{B}_g$ kenne ich einen Beweis des genannten Zerlegungssatzes allerdings nur für den Fall, daß der Koeffizientenring nicht aus den ganzen Zahlen allein, sondern aus allen „ganzzahligen Funktionalen einer Unbestimmten" besteht. (Vgl. dazu die Bemerkung am Schlusse der Einleitung der unmittelbaren vorangehenden Arbeit.)

Die „Eindeutigkeit" der Primfaktorzerlegung bedeutet natürlich hier (und an den entsprechenden Stellen im folgenden) nur „Eindeutigkeit bis auf Einheitsfaktoren".

[3]) Wenn wir von der Zerlegbarkeit eines Elements aus $\mathfrak{A}_g$ ($\mathfrak{A}_r$ usw.) sprechen, meinen wir natürlich „Zerlegbarkeit in $\mathfrak{A}_g$".

[4]) Daß in $\mathfrak{B}_r$ jedes Element eindeutig in Primfaktoren zerlegbar ist, darf wohl als bekannt angesehen werden.

In diesem Zusammenhang ergibt sich nun sofort die weitere Frage:

Gibt es in $\mathfrak{B}_r$ *Reihen* $S^*(x, y)$, *die zwar keiner ganzzahligen Reihe äquivalent sind, wohl aber von* 0 *verschiedene ganzzahlige Reihen teilen*?

Ist diese Frage in bejahendem Sinne zu beantworten, so ist damit endgültig gezeigt, daß es unmöglich ist, unmittelbar aus der Gültigkeit des Zerlegungssatzes in Primelemente für $\mathfrak{B}_r$ auf die Gültigkeit des entsprechenden Zerlegungssatzes für $\mathfrak{B}_g$ zu schließen. — Doch dürfte die Konstruktion einer Reihe $S^*(x, y)$ nicht einfach sein, indessen kann man vielleicht aus dem Bau der Reihe $Q^*(x, y)$ Richtlinien ablesen, nach denen ev. vorzugehen wäre: Charakteristisch für Q^* sind zwei Dinge, nämlich einerseits die starke Zunahme der p-Potenzen in den Nennern der nichtverschwindenden Koeffizienten und andrerseits das Auftreten von „großen Lücken“ (d. h. von vielen Nullen) unter den Koeffizienten. Analysiert man nun unsere früheren Schlüsse genauer, so sieht man, daß die starke Zunahme der Koeffizientennenner allein ausgereicht hätte, um festzustellen, daß Q^* keiner ganzzahligen Reihe äquivalent sein kann. Die Lücken in den Koeffizienten sind notwendig, um zu zeigen, daß das Produkt $Q^* \cdot Q$ auch dann nicht ganzzahlig sein kann, wenn Q mit einer Form einer beliebigen positiven Dimension beginnt. Man könnte in Anbetracht dieser Umstände die Konstruktion von S^* so versuchen, daß man von Q^* oder von einer ähnlich gebauten Reihe ausginge und bei ihr die „Lücken“ in geeigneter Weise „ausfüllte“. Das wäre ein möglicher, wenn auch sonst in keiner Weise sicherer Weg zur Erreichung des gewünschten Zieles.

Eingegangen 7. Juli 1930.

Neuer Beweis und Verallgemeinerung der Tauberschen Sätze, welche die Laplacesche und Stieltjessche Transformation betreffen.

Von *J. Karamata* in Belgrad.

In einer unlängst erschienenen Note beweisen die Herren Hardy und Littlewood [1]) folgende zwei Sätze:

Satz 1. *Es sei $f(t)$ in jedem endlichen Intervall $(0, T)$ und $e^{-st}f(t)$ für jedes $s > 0$ im Intervalle $(0, \infty)$ integrabel. Ist*

$$\int_0^\infty e^{-st} f(t)\,dt \sim As^{-\sigma} \quad bei \quad s \to 0 \qquad (A \geq 0, \quad \sigma > 0)$$

und

$$f(t) \geq 0 \quad für \quad t > 0,$$

so gilt:

$$\int_0^x f(t)\,dt \sim \frac{A}{\Gamma(\sigma+1)}\, x^\sigma \quad bei \quad x \to \infty .$$

Satz 2. *Es sei $f(t)$ in jedem endlichen Intervall $(0, T)$ und $e^{-st}f(t)$ für ein s_0 (und damit für alle $s \geq s_0$) im Intervall $(0, \infty)$ integrabel. Ist*

$$\int_0^\infty e^{-st} f(t)\,dt \sim Bs^{-\sigma} \quad bei \quad s \to \infty \qquad (B \geq 0, \quad \sigma > 0)$$

und

$$f(t) \geq 0 \quad für \quad t > 0,$$

so gilt:

$$\int_0^x f(t)\,dt \sim \frac{B}{\Gamma(\sigma+1)}\, x^\sigma \quad bei \quad x \to 0 .$$

Die beiden Autoren geben keinen direkten Beweis dieser Sätze, sie zeigen nämlich nur, wie sich die beiden Sätze elementar aus einem dritten Satz ableiten lassen, für den sie einen direkten, aber schwierigen Beweis erbringen. Dieser lautet:

Satz 3. *Es sei $f(t)$ in jedem endlichen Intervall $(0, T)$ und $\frac{f(t)}{(t+x)^\varrho}$, wo $\varrho > 0$, für jedes $x > 0$ im Intervall $(0\ \infty)$, integrabel. Ist*

$$\int_0^\infty \frac{f(t)}{(t+x)^\varrho}\,dt \sim Cx^{-\sigma} \qquad \begin{matrix} bei\ x \to \infty \\ bzw.\ bei\ x \to 0 \end{matrix} \qquad (C \geq 0,\ 0 < \sigma < \varrho)$$

[1]) G. H. Hardy and J. E. Littlewood, Notes on the theory of series (XI): On Tauberian theorems. Proc. of the Lond. math. soc. (2) **30** (1929), S. 23—37.

und

$$f(t) \geq 0 \quad \textit{für} \quad t > 0,$$

so gilt:

$$\int_0^\infty f(t)\,dt \sim C\,\frac{\Gamma(\varrho)}{\Gamma(\sigma)\,\Gamma(\varrho-\sigma+1)}\,x^{\varrho-\sigma} \qquad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0. \end{matrix}$$

Kurz nachher zeigte Herr G. Doetsch [2]), daß man umgekehrt den Satz 3 aus den Sätzen 1 und 2 ableiten kann, daß es also genügt, einen direkten Beweis für die Sätze 1 und 2 anzugeben.

Einen solchen direkten Beweis des Satzes 1 hat für die Spezialfälle $\sigma = 0$ und $\sigma = 1$ Herr Doetsch [3]), allgemein Herr O. Szász [4]) mit Hilfe der schwierigen Hardy-Littlewoodschen Methoden gegeben. Diese Methode ist auf Satz 2 nicht anwendbar, andererseits ist nach den Bemerkungen der Herren Doetsch und Hardy-Littlewood Satz 2 nicht aus Satz 1 zu folgern.

Vor kurzer Zeit gab ich [5]) hingegen einen direkten und einfachen Beweis des Satzes 1, welcher sich unverändert zum Beweis des Satzes 2 verwenden läßt.

In der vorstehenden Arbeit werde ich erstens diesen Beweis für die Sätze 1 und 2 gleichzeitig durchführen, indem ich zugleich diese Sätze etwas verallgemeinere, zweitens zeige ich auf eine andere Weise, als es Herr Doetsch getan hat, wie sich Satz 3 aus den Sätzen 1 und 2 (in ihren verallgemeinerten Formen) ableiten läßt. Zum Schluß gebe ich noch die Verallgemeinerung des Satzes 1 in dem Sinne, daß anstelle eines positiven $f(x)$ solche Funktionen in Betracht kommen, welche einer von Herrn R. Schmidt eingeführten Bedingung genügen.

Die Sätze 1 und 2 werden unmittelbar aus dem folgenden Hauptsatz abgeleitet:

Hauptsatz 1. *Es sei $L(x)$ für $x \geq 0$ stetig, positiv und*

$$(1) \qquad \frac{L(ux)}{L(x)} \to 1 \qquad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0 \end{matrix} \qquad \textit{für jedes} \quad u > 0;\ [6])$$

sei ferner

$$e^{-st} f(t) \geq 0 \quad \textit{für} \quad t \geq 0$$

und für jedes $s > 0$ im Intervall $(0, \infty)$ integrabel [7]). *Aus*

$$(2) \qquad \int_0^\infty e^{-st} f(t)\,dt \sim s^{-\sigma} L\left(\frac{1}{s}\right) \qquad \begin{matrix} \textit{bei } s \to 0 \\ \textit{bzw. bei } s \to \infty \end{matrix} \qquad (\sigma \geq 0)$$

folgt dann:

---

[2]) G. Doetsch, Sätze von Tauberschem Charakter im Gebiet der Laplace- und Stieltjes-Transformation. Sitzungsberichte der Preuß. Akad. der Wissenschaften, Phys.-Math. Klasse, 1930, S. 144—157.

[3]) G. Doetsch, Ein Konvergenzkriterium für Integrale. Math. Ann. **82** (1920), S. 68—82.

[4]) O. Szász, Verallgemeinerung und neuer Beweis einiger Sätze Tauberscher Art. Sitzungsberichte der Bayer. Akademie der Wissenschaften 1929, S. 325—340.

[5]) J. Karamata, Neuer Beweis und Verallgemeinerung einiger Tauberian-Sätze, Math. Zeitschrift.

[6]) Stetige und positive Funktionen $L(x)$, welche der Bedingung

$$L(ux)/L(x) \to 1 \text{ bei } x \to \infty \text{ für jedes } u > 0$$

genügen, werde ich von nun ab als langsam wachsende Funktionen bezeichnen (gleichgültig ob sie monoton wachsen oder fallen, oder ob sie zwischen endlichen oder unendlichen Grenzen oszillieren); die Funktionen von der Form $x^\sigma L(x)$ nenne ich hingegen regulär wachsende Funktionen. Diese Terminologie habe ich in meiner Arbeit: „Sur un mode de croissance regulière des fonctions. Mathematica (Cluj, Roumanie) **4** (1930), S. 38—53" angenommen, wo ich diese Funktionen eingehend behandle. Gleichung (1) besagt also, daß $L(x)$ und $L(1/x)$ langsam wachsende Funktionen sind. Siehe diesbezüglich auch I. Schur, Zur Theorie der Cesàroschen und Hölderschen Mittelwerte, Math. Zeitschrift **31** (1929), S. 391—407.

[7]) Der Einfachheit halber wird die Integrabilität im Riemannschen Sinne verstanden.

$$(3)\quad \int_0^\infty e^{-st}\, g(st)\, f(t)\, dt \sim s^{-\sigma}\, L\Big(\frac{1}{s}\Big)\, \frac{1}{\Gamma(\sigma+1)} \int_0^\infty e^{-t}\, g(t)\, d\{t^\sigma\} \qquad \begin{matrix} \textit{bei } s \to 0 \\ \textit{bzw. bei } s \to \infty \end{matrix}$$

für jede beschränkte[8]) *und R-integrable Funktion* $g(t)$. *Für* $\sigma = 0$ *ist unter* t^σ *diejenige Funktion zu verstehen, welche für* $t = 0$ *gleich Null ist, sonst gleich Eins, und* $g(t)$ *soll in diesem Falle für* $t = 0$ *stetig sein.*

Beweis. Setzt man in (2) $s(n+1)$ anstatt s, so ist wegen (1):

$$\int_0^\infty e^{-st}\, e^{-snt}\, f(t)\, dt \sim s^{-\sigma}\, L\Big(\frac{1}{s(n+1)}\Big)\, \frac{1}{(n+1)^\sigma} \sim s^{-\sigma}\, L\Big(\frac{1}{s}\Big)\, \frac{1}{(n+1)^\sigma}$$

$$= s^{-\sigma}\, L\Big(\frac{1}{s}\Big)\, \frac{1}{\Gamma(\sigma+1)} \int_0^\infty e^{-t}\, e^{-nt}\, d\{t^\sigma\},$$

also

$$\int_0^\infty e^{-st}\, P(e^{-st})\, f(t)\, dt \sim s^{-\sigma}\, L\Big(\frac{1}{s}\Big)\, \frac{1}{\Gamma(\sigma+1)} \int_0^\infty e^{-t}\, P(e^{-t})\, d\{t^\sigma\},$$

wo $P(x)$ ein beliebiges Polynom ist. Da sich weiter jeder im Intervalle (0, 1) beschränkten und R-integrablen Funktion $h(x)$ zwei Polynome $P_1(x)$ und $P_2(x)$ derart zuordnen lassen, daß

$$P_1(x) \leq h(x) \leq P_2(x) \quad \text{für} \quad 0 \leq x \leq 1$$

und daß

$$\int_0^\infty e^{-t}\, \{P_2(e^{-t}) - P_1(e^{-t})\}\, d\{t^\sigma\} \leq \varepsilon, \qquad \varepsilon > 0,$$

ausfällt, so folgt die Gleichung (3), in der $h(e^{-t}) = g(t)$ gesetzt worden ist. — In dieser Ausführung bezieht sich das Zeichen „$\sim$“ durchweg auf $s \to 0$, bzw. durchweg auf $s \to \infty$.

Es gilt ein ähnlicher Satz, in dem die Laplacesche Transformierte $\int_0^\infty e^{-st}\, f(t)\, dt$ durch ein Stieltjessches Integral $\int_0^\infty e^{-st}\, d\{A(t)\}$ ausgedrückt wird, nämlich:

Hauptsatz I.[9]). *Es seien* $L(x)$ *und* $L\left(\frac{1}{x}\right)$ *langsam wachsende Funktionen; sei ferner* $A(t)$ *von beschränkter Schwankung, derart daß* $\int_0^\infty e^{-st}\, d\{A(t)\}$ *für jedes* $s > 0$ *exi-*

---

[8]) Die Funktion $g(t)$ braucht nicht immer als beschränkt vorausgesetzt zu sein; wird sie aber in der Umgebung eines Punktes $0 \leqq a \leqq \infty$ nicht beschränkt, so muß sie sich doch so verhalten, daß

$$|g(t)| \leqq G(t) \text{ in der Umgebung von } a \text{ sei,}$$

wo $G(t)$ monoton ins Unendliche wächst, wenn $t \to a$, und

$$\int_0^\infty e^{-t}\, G(t)\, d\{t^\sigma\} \text{ einen Sinn hat.}$$

Hiernach folgt z. B. aus (2):

$$\int_0^\infty e^{-st}\, t^\lambda\, f(t)\, dt \sim s^{-(\sigma+\lambda)}\, L\Big(\frac{1}{s}\Big)\, \frac{\Gamma(\sigma+\lambda)}{\Gamma(\sigma)}, \quad \lambda \geqq 0.$$

[9]) Sein Beweis ist ähnlich dem des Hauptsatzes 1. und findet sich durchgeführt in meiner unter [5]) zitierten Arbeit.

stiert und

$$\int_0^x e^{-st}\,|d\{A(t)\}| = 0\left\{s^{-\sigma}L\left(\frac{1}{s}\right)\right\} \quad \begin{matrix} \text{bei } s\to 0 \\ \text{bzw. bei } s\to\infty \end{matrix} \qquad (\sigma \geqq 0).$$

Aus

$$\text{(4)} \qquad \int_0^x e^{-st}\,d\{A(t)\} \sim s^{-\sigma}L\left(\frac{1}{s}\right) \quad \begin{matrix} \text{bei } s\to 0 \\ \text{bzw. bei } s\to\infty \end{matrix}$$

folgt:

$$\text{(5)} \qquad \int_0^\infty e^{-st}\,g(st)\,d\{A(t)\} \sim s^{-\sigma}L\left(\frac{1}{s}\right)\frac{1}{\Gamma(\sigma+1)}\int_0^\infty e^{-st}\,g(t)\,d\{t^\sigma\} \quad \begin{matrix} \text{bei } s\to 0 \\ \text{bzw. bei } s\to\infty \end{matrix}$$

für jede stetige und beschränkte Funktion $g(t)$. *Für* $\sigma = 0$ *ist unter* t^σ *diejenige Funktion zu verstehen, welche für* $t = 0$ *gleich Null ist, sonst gleich Eins* [10]).

Nun ist es leicht, durch Spezialisierung der Funktion $g(t)$ in den Hauptsätzen die erwähnten Verallgemeinerungen der Sätze 1 und 2 zu gewinnen; setzt man nämlich im Hauptsatze 1

$$\text{(6)} \qquad e^{-t}g(t) = \begin{cases} 1 & \text{für } 0 \leqq t \leqq 1 \\ 0 & \text{für } 1 < t < \infty \end{cases},$$

so ergibt sich, daß aus (2) die Gleichung

$$\int_0^x f(t)\,dt \sim \frac{x^\sigma L(x)}{\Gamma(\sigma+1)} \quad \begin{matrix} \text{bei } x\to 0 \\ \text{bzw. bei } x\to 0 \end{matrix}$$

folgt, was eine Verallgemeinerung der Aussage von Satz 1 und 2 darstellt.

Der Hauptsatz I hingegen gibt den

Satz I—II. *Es seien* $L(x)$ *und* $L(1/x)$ *langsam wachsende Funktionen; es sei ferner* $A(t)$ *nicht abnehmend* [11]), *und* $\int_0^\infty e^{-st}\,d\{A(t)\}$ *habe einen Sinn für jedes* $s > 0$. *Aus*

---

[10]) Im Falle daß $A(t)$ nicht abnimmt, könnte man einen dem Hauptsatze 1 ähnlichen Satz ableiten, nämlich daß aus (4) die Gleichung (5) folgt für jede im Riemann-Stieltjesschen Sinne bezüglich der Funktion $A(t)$ integrable Funktion $g(st)$, nur darf s im allgemeinen Falle nicht alle positiven Werte durchlaufen, damit die Unstetigkeiten der Funktionen $g(st)$ und $A(t)$ nicht zusammenfallen. Ist $A(t)$ stetig, so fällt diese Bedingung weg.

[11]) Es sei schon hier bemerkt, daß in dem Falle, wo $x^\sigma L(x)\to\infty$ bei $x\to\infty$ (der Einfachheit halber betrachte ich hier nur den Fall, wo $x\to\infty$), die Bedingung der Monotonie der Funktion $A(t)$ durch eine geringere ersetzt werden kann. Es ist nämlich leicht einzusehen, daß Satz I noch gilt, wenn eine Funktion $B(t)$ existiert, so daß $A(t) + B(t)$ nicht abnimmt, d. h.

$$A(t+h) - A(t) > -\{B(t+h) - B(t)\} \text{ für } h > 0,$$

und

$$\text{(I)} \qquad B(x) \sim bx^\sigma L(x) \text{ bei } x\to\infty,\ b > 0.$$

Diese Bedingung enthält z. B. die folgende:

$$\text{(II)} \qquad A(x+h) - A(x) = O_L\{(x+h)^\sigma L(x+h) - x^\sigma L(x)\},\ h > 0;$$

oder: Wenn $A(x)$ eine Ableitung besitzt und die Ableitung von $x^\sigma L(x)$ ebenfalls regulär wachsend ist ($\sigma > 0$), so kann die Bedingung (II) durch die folgende ersetzt werden:

$$\text{(III)} \qquad A'(x) = O_L\{x^{\sigma-1}L(x)\},\ \sigma > 0.$$

Dies ist richtig, weil in diesem Falle

$$\{x^\sigma L(x)\}' \sim \sigma x^{\sigma-1}L(x)$$

(siehe meine unter [6]) zitierte Note S. 51, Abschnitt 7), also wegen (III) $A'(x) = O_L\{[x^\sigma L(x)]'\}$, was durch Integration (II) ergibt.

Andererseits ist leicht einzusehen, daß aus der Bedingung (I)

$$\liminf_{x=\infty} \operatorname{Min}_{x\leqq t\leqq\lambda x} \frac{A(t) - A(x)}{x^\sigma L(x)} > -b(\lambda^\sigma - 1)\to 0 \quad \text{bei} \quad 1 < \lambda \to 1$$

$$\int_0^\infty e^{-st}\, d\{A(t)\} \sim s^{-\sigma} L\left(\frac{1}{s}\right) \quad \begin{matrix} \textit{bei } s \to 0 \\ \textit{bzw. bei } s \to \infty \end{matrix}$$

folgt dann:

$$A(x) \sim \frac{x^\sigma L(x)}{\Gamma(\sigma+1)} \quad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0\,. \end{matrix}$$

Dieser Satz kann nach der Bemerkung unter [10]) mit derselben speziellen Funktion (6) gewonnen werden. Eine direkte Zurückführung des Satzes I—II auf den Hauptsatz I ist im Falle $s \to 0$, $x \to \infty$ in meiner unter [5]) zitierten Arbeit bewerkstelligt.

Um nun noch die entsprechende Verallgemeinerung des Satzes 3 nämlich:

Satz III. *Es seien $L(x)$ und $L(1/x)$ langsam wachsende Funktionen, sei ferner $A(t)$ nicht abnehmend und existiere das Integral*

$$\int_0^\infty \frac{d\{A(t)\}}{(t+x)^\varrho} \quad \textit{für jedes } x > 0 \quad (\varrho \geqq 0).$$

Aus

$$\int_0^\infty \frac{d\{A(t)\}}{(t+x)^\varrho} \sim x^{-\sigma} L(x) \quad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0 \end{matrix} \quad (0 \leqq \sigma \leqq \varrho)$$

folgt dann:

$$(7) \qquad A(x) \sim \frac{\Gamma(\varrho)}{\Gamma(\sigma)\,\Gamma(\varrho-\sigma+1)}\, x^{\varrho-\sigma} L(x) \quad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0\,. \end{matrix}$$

aus Satz I—II abzuleiten, beweise ich zunächst den folgenden

Hauptsatz II. *Es seien $L(x)$ und $L(1/x)$ langsam wachsende Funktionen; sei ferner $A(t)$ nicht abnehmend und existiere das Integral*

$$\int_0^\infty \frac{d\{A(t)\}}{(t+x)^\varrho} \quad \textit{für jedes } x > 0 \quad (\varrho \geqq 0).$$

Aus

$$(8) \qquad \int_0^\infty \frac{d\{A(t)\}}{(t+x)^\varrho} \sim x^{-\sigma} L(x) \quad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0 \end{matrix} \quad (0 \leqq \sigma \leqq \varrho)$$

folgt dann:

$$(9) \quad \int_0^\infty G\left(\frac{t}{x}\right) d\{A(t)\} \sim x^{\varrho-\sigma} L(x)\, \frac{\Gamma(\varrho)}{\Gamma(\sigma)} \int_0^\infty e^{-t}\, g(t)\, t^{\sigma-1}\, dt \quad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0, \end{matrix}$$

wo

$$G(y) = \int_0^\infty e^{-y\zeta} e^{-\zeta}\, g(\zeta)\, \zeta^{\varrho-1}\, d\zeta,$$

---

folgt, so daß die Bedingung

$$(IV) \qquad \liminf_{x=\infty} \operatorname{Min}_{x \leqq t \leqq x\lambda} \frac{A(t)-A(x)}{x^\sigma L(x)} > -w(\lambda) \to 0 \quad \text{bei} \quad 1 < \lambda \to 1,$$

eine geringere als die Bedingung (I) ist. Die Bedingung (IV) ist hingegen diejenige, welche im Gebiet der Laplaceschen Transformation derjenigen entspricht, die Herr R. Schmidt in seiner Arbeit „Über divergente Folgen und lineare Mittelbildungen, Math. Zeitschrift **22** (1925), S. 89—159" betrachtet.

Es besteht nun die Frage, ob auch umgekehrt (I) aus (IV) folgt, in welchem Falle der Satz I, wo die Bedingung der Monotonie der Funktion $A(t)$ durch (IV) ersetzt ist, bei $x^\sigma L(x) \to \infty$ schon bewiesen wäre.

und $g(t)$ eine beliebige beschränkte und R-integrable Funktion ist. [*Für $\sigma = 0$ bedeutet die rechte Seite von* (9) $\Gamma(\varrho) x^{\varrho} L(x) g(0)$].

Beweis. Setzt man im Integral (8)

$$\frac{1}{(t+x)^{\varrho}} = \frac{1}{\Gamma(\varrho)} \int_0^{\infty} e^{-t\tau} e^{-x\tau} \tau^{\varrho-1} d\tau,$$

und ersetzt in derselben Gleichung x durch $x(1+n)$, so folgt:

$$\int_0^{\infty}\int_0^{\infty} e^{-t\tau} e^{-x\tau} P(e^{-x\tau})\, \tau^{\varrho-1} d\tau\, d\{A(t)\} \sim \frac{\Gamma(\varrho)}{\Gamma(\sigma)} x^{-\sigma} L(x) \int_0^{\infty} e^{-t} P(e^{-t})\, t^{\sigma-1} dt$$

woraus sich wie bei dem Hauptsatz I ergibt:

$$\int_0^{\infty}\int_0^{\infty} e^{-t\tau} e^{-x\tau} h(e^{-x\tau})\, \tau^{\varrho-1} d\tau\, d\{A(t)\} \sim x^{-\sigma} L(x) \frac{\Gamma(\varrho)}{\Gamma(\sigma)} \int_0^{\infty} e^{-t} h(e^{-t})\, t^{\sigma-1} dt.$$

Diese Gleichung geht durch die Substitutionen

$$h(e^{-t}) = g(t), \quad \tau x = \zeta$$

in (9) über, was Hauptsatz II beweist.

Wird nun im Hauptsatze II $g(t)$ so gewählt, daß

$$e^{-t} g(t)\, t^{\varrho-1} = \begin{cases} 0 & \text{für} \quad 0 < t < 1 \\ 1 & \text{für} \quad 1 < t < 1+\varepsilon \\ 0 & \text{für} \quad 1+\varepsilon < t < \infty, \end{cases}$$

und $1/x = s$ gesetzt, so geht Gleichung (9) über in

$$\int_0^{\infty} e^{-st} \frac{1 - e^{-st\varepsilon}}{st\varepsilon} d\{A(t)\} \sim s^{-(\varrho-\sigma)} L\left(\frac{1}{s}\right) \frac{\Gamma(\varrho)}{\Gamma(\sigma)} \cdot \frac{(1+\varepsilon)^{\sigma-\varrho+1} - 1}{(\sigma-\varrho+1)\varepsilon},$$

und da in dieser Gleichung der Grenzübergang $\varepsilon \to 0$ gemacht werden kann, so folgt:

$$\int_0^{\infty} e^{-st} d\{A(t)\} \sim s^{-(\varrho-\sigma)} L\left(\frac{1}{s}\right) \frac{\Gamma(\varrho)}{\Gamma(\sigma)};$$

diese Gleichung führt Satz III auf Satz I—II zurück.

In vorstehender Ausführung bezieht sich das Zeichen „$\sim$“ entweder durchweg auf

$$x \to \infty, \quad s \to 0 \quad \text{oder durchweg auf} \quad x \to 0, \quad s \to \infty.$$

Es sei hier noch erwähnt, daß sich Satz III noch dadurch verallgemeinern läßt, daß man auch der im Integrale (8) vorkommenden Funktion $\frac{1}{(x+t)^{\varrho}}$ einen langsam wachsenden Faktor $L_1(x+t)$ zusetzt, in dem Sinne, daß man im erwähnten Integral diese Funktion durch eine allgemeinere ersetzt, nämlich durch

$$w(x+t) = \int_0^{\infty} e^{-(x+t)\zeta} \varphi(\zeta)\, d\zeta,$$

wo $\varphi(t) = t^{\varrho-1} l(t)$ eine regulär wachsende Funktion ist. Das zeigt der folgende Satz:

Satz IV. *Seien $L(x)$, $L\left(\frac{1}{x}\right)$, $L_1(x)$, $L_1\left(\frac{1}{x}\right)$ langsam wachsende Funktionen, und sei $1/x^{\varrho} L_1(x)$, $\varrho \geq 0$, die Laplacesche Transformierte der regulär wachsenden Funktion $\varphi(x) = x^{\varrho-1} l(x)$, das heißt:*

$$w(x) = \frac{1}{x^{\varrho} L_1(x)} = \int_0^{\infty} e^{-x\zeta} \varphi(\zeta)\, d\zeta;$$

sei ferner $A(t)$ nicht abnehmend und existiere das Integral

$$V(x) = \int_0^\infty w(x+t)\, d\{A(t)\} \quad \textit{für jedes} \quad x > 0.$$

Aus

$$V(x) \sim x^{-\sigma} L(x) \qquad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0 \end{matrix} \tag{10}$$

folgt dann:

$$A(x) \sim \frac{\Gamma(\varrho)}{\Gamma(\sigma)\,\Gamma(\varrho-\sigma+1)}\, x^{\varrho-\sigma} L(x) L_1(x) \qquad \begin{matrix} \textit{bei } x \to \infty \\ \textit{bzw. bei } x \to 0. \end{matrix}$$

Da der Beweis fast derselbe, wie derjenige des Satzes III ist, so sei er hier nur in Kürze dargelegt.

Aus (10) folgt wie beim Beweis des Hauptsatzes II:

$$\int_0^\infty W_\varrho(x,t)\, d\{A(t)\} \sim x^{-\sigma} L(x) \frac{1}{\Gamma(\sigma)} \int_0^\infty e^{-t}\, g(t)\, t^{\sigma-1}\, dt, \tag{11}$$

wo

$$W_\varrho(x,t) = \int_0^\infty e^{-t\zeta} e^{-x\zeta}\, g(x\zeta)\, \varphi(\zeta)\, d\zeta.$$

Ist nun

$$e^{-t} g(t) = \begin{cases} 0 & \text{für} \quad 0 < t < 1 \\ 1 & \text{für} \quad 1 < t < 1+\varepsilon \\ 0 & \text{für} \quad 1+\varepsilon < t < \infty, \end{cases}$$

so wird

$$W_\varrho(x,t) = \int_{\frac{1}{x}}^{\frac{1+\varepsilon}{x}} e^{-t\zeta}\, \varphi(\zeta)\, d\zeta.$$

(11) ergibt also, indem man $\eta = x\zeta$ setzt und durch ε/x dividiert:

$$\int_0^\infty d\{A(t)\}\, \frac{1}{\varepsilon} \int_1^{1+\varepsilon} e^{-\frac{t}{x}\eta}\, \varphi\left(\frac{\eta}{x}\right) d\eta \sim x^{1-\sigma} L(x)\, \frac{1}{\Gamma(\sigma)} \cdot \frac{(1+\varepsilon)^\sigma - 1}{\sigma\varepsilon},$$

woraus, wenn $\varepsilon \to 0$, $x = 1/s$ und $\varphi(x) = x^{\varrho-1} l(x) \sim \dfrac{x^{\varrho-1}}{\Gamma(\varrho)\, L_1(1/x)}$ gesetzt wird, folgt:

$$\int_0^\infty e^{-st}\, d\{A(t)\} \sim s^{-(\varrho-\sigma)}\, \frac{\Gamma(\varrho)}{\Gamma(\sigma)}\, L\left(\frac{1}{s}\right) L_1\left(\frac{1}{s}\right).$$

Hieraus erhält man auf Grund von Satz I—II die Behauptung. — Im vorstehenden Beweis bezieht sich wieder das Zeichen „$\sim$“ auf $x \to \infty$, $s \to 0$, bzw. auf $x \to 0$, $s \to \infty$.

Ich gehe noch zu der Verallgemeinerung des Satzes 1 oder I über (ähnliche Schlüsse sind auf die Sätze 2 und 3 anwendbar), welche am Anfang und unter [11]) schon erwähnt war, und in welcher also die Monotonie der Funktion $A(t)$ durch die Bedingung (IV) im Zitat [11]) ersetzt wird; dieser Satz lautet:

Satz A. *Es sei die Funktion $L(x)$ für $x \geq 0$ stetig, positiv und*

$$L(ux)/L(x) \to 1 \quad \textit{bei} \quad x \to \infty \quad \textit{für jedes} \quad u > 0;$$

sei ferner $A(x)$ von beschränkter Schwankung und existiere das Integral

$$\int_0^\infty e^{-st}\, d\{A(t)\} \quad \textit{für jedes} \quad s > 0.$$

Aus

$$\int_0^\infty e^{-st}\, d\{A(t)\} \sim s^{-\sigma} L\left(\frac{1}{s}\right) \quad bei \quad s \to 0, \quad \sigma \geqq 0, \tag{12}$$

und

$$\liminf_{x=\infty} \operatorname{Min}_{x \leqq t \leqq \lambda x} \frac{A(t) - A(x)}{x^\sigma L(x)} > -w(\lambda) \to 0 \quad bei \quad 1 < \lambda \to 1, \tag{13}$$

folgt:

$$A(x) \sim x^\sigma L(x) \quad bei \quad x \to \infty. \tag{14}$$

Den Beweis dieses Satzes führe ich auf die zwei folgenden zurück:

Satz B. *Sei $L(x)$ langsam wachsend, sei ferner $A(x)$ von beschränkter Schwankung und existiere das Integral*

$$\int_0^\infty e^{-st}\, d\{A(t)\} \quad für \ jedes \quad s > 0.$$

Aus

$$\int_0^\infty e^{-st}\, d\{A(t)\} \sim s^{-\sigma} L\left(\frac{1}{s}\right) \quad bei \quad s \to 0, \quad \sigma \geqq 0,$$

und

$$A(x) = O_L\{x^\sigma L(x)\} \quad bei \quad x \to \infty \tag{15}$$

folgt:

$$\frac{1}{x}\int_0^x A(t)\, dt \sim x^\sigma L(x) \quad bei \quad x \to \infty. \tag{16}$$

Satz C. *Sei $L(x)$ langsam wachsend, und $A(t)$ R-integrabel.*

Aus

$$\frac{1}{x}\int_0^x A(t)\, dt \sim x^\sigma L(x), \quad bei \quad x \to \infty, \quad \sigma \geqq 0, \tag{16}$$

und

$$\liminf_{x=\infty} \operatorname{Min}_{x \leqq t \leqq x\lambda} \frac{A(t) - A(x)}{x^\sigma L(x)} > -w(\lambda) \to 0 \quad bei \quad 1 < \lambda \to 1, \tag{13}$$

folgt:

$$A(x) \sim x^\sigma L(x) \quad bei \quad x \to \infty.$$

Der Satz B folgt aus der Bemerkung unter [11]), Bedingung (III), da

$$\int_0^\infty e^{-st}\, d\{A(t)\} = s\int_0^\infty e^{-st}\, d\left\{\int_0^t A(\tau)\, d\tau\right\},$$

wenn $A(0) = 0$ gesetzt wird, also wegen (12)

$$\int_0^\infty e^{-st}\, d\left\{\int_0^t A(\tau)\, d\tau\right\} \sim s^{-(\sigma+1)} L\left(\frac{1}{s}\right) \quad \text{bei} \quad s \to 0,$$

woraus unter der Bedingung (15) die Gleichung (16) folgt.

Der Satz bleibt sogar richtig bei $\sigma > -1$.

Um Satz C zu beweisen, bemerke ich zuerst, daß es genügt, statt (16) die folgende Gleichung:

$$\int_0^x A(t)\, dt = o\{x^{\sigma+1} L(x)\} \quad bei \quad x \to \infty \tag{17}$$

vorauszusetzen (da man nur statt $A(x)$ die Funktion $A(x) - x^\sigma L(x)$ zu betrachten hätte) und daß aus (17)

$$(18) \qquad \int_x^{x\lambda} A(t)\,dt = o\{x^{\sigma+1}L(x)\} \quad \text{bei} \quad x \to \infty, \quad \lambda > 1$$

folgt.

Nun ist

a) $$\limsup_{x=\infty} \frac{A(x)}{x^\sigma L(x)} \leq 0.$$

Denn weil auf Grund von (18)

$$-x(\lambda-1)A(x) = \int_x^{x\lambda}\{A(t)-A(x)\}dt + o\{x^{\sigma+1}L(x)\} \geq x(\lambda-1)\operatorname*{Min}_{x\leqq t\leqq x\lambda}\{A(t)-A(x)\} + o\{x^{\sigma+1}L(x)\}$$

ist, so wird nach (13)

$$\limsup_{x=\infty} \frac{A(x)}{x^\sigma L(x)} < w(\lambda) \to 0 \quad \text{bei} \quad \lambda \to 1,$$

was a) beweist.

b) $$M(x) = \operatorname*{Max}_{x\leqq t\leqq x\lambda} \frac{A(t)}{t^\sigma L(t)} \to 0 \quad \text{bei} \quad x \to \infty.$$

Denn findet dies nicht statt, so existiert eine Zahl $-M$, $M > 0$, und eine Folge x_ν-Werte, derart daß

$$M(x_\nu) \to -M \quad \text{bei} \quad x_\nu \to \infty;$$

dann wird aber

$$\frac{1}{x_\nu^{\sigma+1}L(x_\nu)}\int_{x_\nu}^{x_\nu\lambda} A(t)dt \leq \frac{M(x_\nu)}{x_\nu^{\sigma+1}L(x_\nu)}\int_{x_\nu}^{x_\nu\lambda} t^\sigma L(t)\,dt \to \frac{-M}{\sigma+1}(\lambda^{\sigma+1}-1) \quad \text{bei} \quad x\to\infty\ ^{12}),$$

was (18) wiederspricht.

c) $$\liminf_{x=\infty} \frac{A(x)}{x^\sigma L(x)} \geq 0.$$

Es sei x_μ derart, daß

$$\frac{A(x_\mu)}{x_\mu^\sigma L(x_\mu)} = M(x);$$

dann ist wegen (13) und b)

$$\liminf_{x_\mu=\infty} \frac{A(t)-A(x_\mu)}{x_\mu^\sigma L(x_\mu)} = \liminf_{x_\mu=\infty} \frac{A(t)}{x_\mu^\sigma L(x_\mu)} > -w(\lambda), \quad x_\mu \leqq t \leqq \lambda x_\mu,$$

das heißt

$$\liminf_{x_\mu=\infty} \frac{A(t)}{t^\sigma L(t)} \geq 0, \quad x_\mu \leq t \leq x_\mu\lambda,$$

und da t bei $x_\mu \to \infty$ beliebig gegen Unendlich streben kann, so folgt c).

Wegen a) und c) ist der Satz C bewiesen [13]).

---

[12]) Siehe meine unter [6]) zitierte Note, S. 40.

[13]) Es sei hier noch bemerkt, daß dieser Beweis fast unverändert bleibt, wenn die Bedingung (13) durch die folgende:

$$\liminf_{x=\infty} \operatorname*{Min}_{x\leqq t\leqq\lambda x}\left\{\frac{A(t)}{t^\sigma L(t)} - \frac{A(x)}{x^\sigma L(x)}\right\} > -w(\lambda) \to 0 \text{ bei } 1<\lambda\to 1$$

ersetzt wird.

Die Zurückführung des Satzes A auf die Sätze B und C ist im Falle $\sigma > 0$ besonders leicht, da schon aus der Bedingung (13) die Bedingung (15) folgt. Ist nämlich

$$A(x\lambda) - A(x) > - Mx^\sigma L(x), \quad \lambda > 1, \quad M > 0, \quad \sigma > 0,$$

so wird

$$A(x) = \sum_{\nu=0}^{\infty} \{A(x\lambda^{-\nu}) - A(x\lambda^{-\nu-1})\} > - M \sum_{\nu=0}^{\infty} x^\sigma \lambda^{-(\nu+1)\sigma} L(x\lambda^{-(\nu+1)\sigma}) =$$

$$= - M x^\sigma L(x) \sum_{\nu=0}^{\infty} \left(\frac{1}{\lambda^\sigma}\right)^{\nu+1} \frac{L(x/\lambda^{\nu+1})}{L(x)},$$

das heißt

$$A(x) \geq \frac{- M}{\lambda^\sigma - 1} x^\sigma L(x)\{1 + \varepsilon(x)\}, \quad \text{wo} \quad \varepsilon(x) \to 0 \quad \text{bei} \quad x \to \infty.$$

Dies besagt also, daß (15) aus (13) folgt, so daß im Falle $\sigma > 0$ die aufeinanderfolgende Anwendung der Sätze B und C den Satz A beweist.

Der Fall, wo $\sigma = 0$ ist, bietet größere Schwierigkeiten dar, da

$$A(t) - A(x) > - M L(x), \quad \lambda > 1, \quad x \leq t \leq x\lambda,$$

nicht notwendig die einseitige Beschränktheit von $\frac{A(x)}{L(x)}$ nach sich zieht. Man könnte sich hingegen des folgenden Hilfssatzes bedienen:

Hilfsatz. *Aus*

$$\int_0^{\infty} e^{-st}\, d\{A(t)\} = O\left\{L\left(\frac{1}{s}\right)\right\} \quad \textit{bei} \quad s \to 0$$

und

$$A(t) - A(x) > - ML(x), \quad \lambda > 1, \quad x > t \leq x\lambda$$

folgt:

$$A(x) = O_L\{L(x)\} \quad \textit{bei} \quad x \to \infty \text{ [14]}.$$

Hier gebe ich aber einen andern Beweis, der von folgendem, den Tauberschen o-Sätzen entsprechenden Satz Gebrauch macht:

Satz D. *Es sei $L(x)$ langsam wachsend, sei ferner $B(t)$ von beschränkter Schwankung und existiere das Integral $\int_0^{\infty} e^{-st}\, d\{B(t)\}$ für jedes $s > 0$.*

Aus

$$\int_0^{\infty} e^{-st}\, d\{B(t)\} \sim L\left(\frac{1}{s}\right) \quad \textit{bei} \quad s \to 0 \tag{19}$$

und

$$B(x\lambda) - B(x) = o\{L(x)\} \quad \textit{bei} \quad x \to \infty, \quad \lambda > 1, \tag{20}$$

folgt:

$$B(x) \sim L(x) \quad \textit{bei} \quad x \to \infty. \tag{21}$$

Beweis. Ist $y = x\lambda^p$, $\lambda > 1$, p *ganz*, und wegen (20)

$$|B(t\lambda) - B(t)| < \varepsilon_1(t) L(t), \quad \text{wo} \quad \varepsilon_1(t) \to 0 \quad \text{bei} \quad t \to \infty,$$

so wird

---

[14]) Diese Beweisanordnung wäre diejenige, welche Herr T. Vijayaraghavan in „A Tauberian theorem, Journal London Math. Soc. **1** (1926), S. 113—120" für Potenzreihen gegeben hat.

$$|B(y)-B(x)| = \left|\sum_{\nu=1}^{p}\left\{B\left(\frac{y}{\lambda^\nu}\,\lambda\right)-B\left(\frac{y}{\lambda^\nu}\right)\right\}\right| \leq \sum_{\nu=1}^{p}\varepsilon_1\left(\frac{y}{\lambda^\nu}\right)L\left(\frac{y}{\lambda^\nu}\right)$$
$$= L(y)\cdot\lg\left(\frac{y}{x}\right)\frac{1}{\lg\lambda}\cdot\frac{1}{p}\sum_{\nu=1}^{p}\varepsilon_1(y\lambda^{-\nu})\,\frac{L(y\lambda^{-\nu})}{L(y)},$$

das heißt

(22) $|B(y)-B(x)| \leq L(y)\lg\left(\frac{y}{x}\right)\varepsilon(y)$, wo $\varepsilon(y)\to 0$ bei $y\to\infty$ [15]).

Daraus folgt, wenn $x=\frac{1}{s}$ und

$$B(x)-\int_0^x e^{-st}d\{B(t)\} = (1-e^{-1})B(x) - s\int_0^x e^{-st}B(t)\,dt = s\int_0^x e^{-st}\{B(x)-B(t)\}dt$$

gesetzt wird, daß

$$|B(x)-\int_0^x e^{-st}d\{B(t)\}| \leq \varepsilon(x)L(x)s\int_0^x \lg\left(\frac{x}{t}\right)dt = \varepsilon(x)L(x)\int_0^1 \lg\left(\frac{1}{t}\right)dt,$$

das heißt

(23) $$B(x)-\int_0^x e^{-st}d\{B(t)\} = o\{L(x)\} \quad \text{bei} \quad x=\frac{1}{s}\to\infty.$$

Weiter wird

$$\left|\int_x^\infty e^{-st}d\{B(t)\}\right| \leq \sum_{\nu=1}^{\infty}\left|\int_{x\lambda^\nu}^{x\lambda^{\nu+1}} e^{-st}d\{B(t)\}\right| \leq \sum_{\nu=1}^{\infty} e^{-\lambda^\nu}|B(t_\nu)-B(x\lambda^\nu)| \leq L(x)\sum_{\nu=1}^{\infty}e^{-\lambda^\nu}\varepsilon_\nu(x\lambda^\nu),$$

$$\text{wo} \quad x\lambda^\nu \leq t_\nu \leq x\lambda^{\nu+1} \quad \text{und} \quad \varepsilon_\nu(x)\to 0 \quad \text{bei} \quad x\to\infty,$$

da, wie schon unter [15]) bemerkt war, die Gleichung (20) gleichmäßig in λ besteht. Es ist also

$$\int_x^\infty e^{-st}d\{B(t)\} = o\{L(x)\} \quad \text{bei} \quad x=1/s\to\infty,$$

woraus wegen (23)

$$B(x)-\int_0^\infty e^{-st}d\{B(t)\} = o\{L(x)\} \quad \text{bei} \quad x=1/s\to\infty,$$

welche Gleichung zusammen mit (19) die Gleichung (21) ergibt.

Sei nun

(24) $$\int_0^\infty e^{-st}d\{A(t)\} \sim L\left(\frac{1}{s}\right) \quad \text{bei} \quad s\to 0;$$

daraus folgt, wenn t durch $t\lambda$ ersetzt wird:

$$\int_0^\infty e^{-s\lambda t}d\{A(t\lambda)\} \sim L\left(\frac{1}{s}\right) \sim L\left(\frac{1}{s\lambda}\right) \quad \text{bei} \quad s\to 0,$$

also

$$\int_0^\infty e^{-st}d\{A(\lambda t)-A(t)\} = o\left\{L\left(\frac{1}{s}\right)\right\} \quad \text{bei} \quad s\to 0.$$

Da wegen (13) (für $\sigma=0$)

[15]) Nach der Eigenschaft der langsam wachsenden Funktionen, daß

$$L(\lambda x)\sim L(x) \text{ bei } x\to\infty \text{ für jedes } \lambda>0$$

gleichmäßig in bezug auf $\lambda>\varepsilon>0$ besteht, ist auch (20) wegen (22) gleichmäßig in λ.

$$A(\lambda t) - A(t) = o\{L(t)\} \quad \text{bei} \quad t \to \infty,$$

ist, so folgt nach Satz B:

$$B(\lambda x) - B(x) = o\{L(x)\} \quad \text{bei} \quad x \to \infty,$$

wo

$$B(x) = \frac{1}{x}\int_0^x A(t)\,dt, \tag{25}$$

gesetzt worden ist.

Weiter folgt aus (24)):

$$\int_0^\infty e^{-st}\,d\{A(t)\} = s\int_0^\infty e^{-st}A(t)\,dt = s^2\int_0^\infty e^{-st}tB(t)\,dt \sim L\left(\frac{1}{s}\right) \quad \text{bei} \quad s \to 0,$$

woraus folgt:

$$\int_0^\infty e^{-st}B(t)\,dt \sim \int_s^\infty L\left(\frac{1}{t}\right)\frac{dt}{t^2};\ ^{16})$$

beachtet man, daß

$$\int_s^\infty L\left(\frac{1}{t}\right)\frac{dt}{t^2} = \int_0^x L(t)\,dt \sim xL(x) \quad \text{bei} \quad x = 1/s \to \infty\ ^{17})$$

ist, so wird

$$s\int_0^\infty e^{-st}B(t)\,dt = \int_0^\infty e^{-st}\,d\{B(t)\} \sim L\left(\frac{1}{s}\right) \quad \text{bei} \quad s \to 0.$$

Aus dieser Gleichung und Gleichung (25) folgt endlich nach Satz D, daß

$$B(x) = \frac{1}{x}\int_0^x A(t)\,dt \sim L(x) \quad \text{bei} \quad x \to \infty,$$

also nach Satz C

$$A(x) \sim L(x) \quad \text{bei} \quad x \to \infty,$$

was Satz A vollständig beweist.

Was die Bedingung (13) des Satzes A betrifft, so war schon unter [13]) bemerkt, daß sie im Satze C durch die folgende:

$$\lim_{x=\infty}\ \inf_{x<t\leqq x\lambda}\ \mathrm{Min}\left\{\frac{A(t)}{t^\sigma L(t)} - \frac{A(x)}{x^\sigma L(x)}\right\} > -w(\lambda) \to 0 \quad \text{bei} \quad 1 < \lambda \to 1 \tag{26}$$

ersetzt werden kann. Dies kann auch im Satz A geschehen, man braucht nur zu bemerken, daß Satz D noch giltig bleibt, wenn die Bedingung (20) durch

$$B(\lambda x) - B(x) \sim (\lambda^\sigma - 1)\,x^\sigma L(x) \quad \text{bei} \quad x \to \infty$$

und $L(x)$ durch $x^\sigma L(x)$ ersetzt wird.

Was die beiden Bedingungen (13) und (26) anbelangt, so kann bemerkt werden, daß (26) nicht mehr (wie es (13) tut) die einseitige Beschränktheit von $\frac{A(x)}{x^\tau L(x)}$ nach sich zieht. Aus (13) aber folgt auch (26) nicht. Hingegen kann man zeigen, daß aus

---

[16]) Das folgt aus dem von O. Stolz, Grundzüge der Diff. und Integralrechnung, Bd. 1 (1893), S. 72—77, präzisierten de L'Hôpitalschen Satz.

[17]) Siehe in meiner unter [6]) zitierten Note, S. 40, oder 47.

$$(27)\qquad \limsup_{x=\infty} \operatorname{Max}_{x<t\leqq\lambda x} \left|\frac{A(t)-A(x)}{x^\sigma L(x)}\right| < u(\lambda) \to 0 \quad \text{bei} \quad 1<\lambda\to 1$$

die Ungleichung

$$(28)\qquad \limsup_{x=\infty} \operatorname{Max}_{x<t\leqq\lambda x} \left|\frac{A(t)}{t^\sigma L(t)} - \frac{A(x)}{x^\sigma L(x)}\right| < 2w(\lambda) \to 0 \quad \text{bei} \quad 1<\lambda\to 1$$

folgt, da sich aus (27)

$$\limsup_{x=\infty} \left|\frac{A(x)}{x^\sigma L(x)}\right| < \frac{w(\lambda)}{\lambda^\sigma - 1}$$

ergibt, weshalb wegen (27) und

$$\frac{A(t)}{t^\sigma L(t)} - \frac{A(x)}{x^\sigma L(x)} = \frac{A(t)-A(x)}{x^\sigma L(x)} + \frac{A(t)}{t^\sigma L(t)}\left\{1 - \frac{t^\sigma L(t)}{x^\sigma L(x)}\right\}$$

(28) folgt.

Die Beziehung zwischen den Bedingungen (13) und (26) ist aber deutlich aus dem folgenden zu ersehen:

Sei $l_0(x)$ die von Herrn R. Schmidt [18]) eingeführte *langsam oszillierende Funktion* d. h.

$$\limsup_{x=\infty} |l_0(t) - l_0(x)| < w(\lambda) \to 0 \quad \text{bei} \quad 1<\lambda\to 1, \quad x \leqq t \leqq x\lambda,$$

sie werde mit $\bar{l}_0(x)$ bezeichnet, wenn sie beschränkt ist; $m(x)$ sei eine beliebige nicht abnehmende Funktion; genügt dann die Funktion $A(x)$ der Bedingung (13), so kann sie in die Form gesetzt werden:

$$A(x) = x^\sigma L(x)\, \bar{l}_0(x) + m(x);$$

wenn dagegen $A(x)$ der Bedingung (26) genügt, so wird

$$A(x) = x^\sigma L(x)\, l_0(x) + x^\sigma L(x)\, m(x),$$

woraus nun ersichtlich ist, daß diejenige Funktion, welche diese beiden enthält, die Form

$$A(x) = x^\sigma L(x)\, l_0(x) + m(x),$$

haben muß, in welchem Falle aber die Giltigkeit des Satzes A noch zu prüfen wäre.

Zum Schluß sei noch erwähnt, daß der Satz A auf Dirichletsche Reihen angewendet, d. h. wenn man setzt:

$$A(x) = \begin{cases} 0 & \text{für} \quad 0 \leq x \leq \lambda_1, \\ a_1 + a_2 + \cdots + a_n & \text{für} \quad \lambda_n < x \leq \lambda_{n+1}, \quad (n = 1, 2 \ldots), \end{cases}$$

neu ist. Hingegen ist er für Potenzreihen schon von Herrn R. Schmidt [19]) bewiesen worden, doch sind die Ergebnisse des Herrn Schmidt im Falle $\sigma = 0$ etwas geringer als das, was Satz A liefert, da der von ihm eingeführten *gestrahlten Funktion* $s(x)$ (welche im Falle $\sigma > 0$ mit der regulär wachsenden Funktion identisch ist) eine nicht abnehmende Funktion, *Vergleichsfunktion*, $\sigma(x)$ entspricht, so daß $s(x) \sim \sigma(x)$, eine Bedingung, welche die langsam wachsenden Funktionen im allgemeinen nicht erfüllen; diese dürfen sogar zwischen endlichen oder unendlichen Grenzen oszillieren.

---

[18]) Siehe l. c. [11]) S. 127—142.

[19]) Siehe l. c. [11]) S. 151.

Eingegangen 13. August 1930.

The condition for integer solutions of $ax^2 + by^2 + cz^2 + dt^2 = 0$.

Von *L. J. Mordell* in Manchester.

§ 1. The necessary and sufficient conditions for the solvability of

$$ax^2 + by^2 + cz^2 + dt^2 = 0, \tag{1}$$

where a, b, c, d are given integers, none of which is zero, and x, y, z, t are unknown integers not all zero, were first given by Meyer[1]) in 1884. Some assumptions can be made which simplify the problem without loss of generality. Thus it may be supposed that a, b, c, d are all free from squared factors > 1. For if

$$a = a'p^2,\ b = b'q^2,\quad c = c'r^2,\ d = d's^2,$$

a correspondence can be established between the solutions of (1) and of

$$a'x'^2 + b'y'^2 + c'z'^2 + d't'^2 = 0$$

by means of

$$x' = px,\quad y' = qy,\quad z' = rz,\quad t' = st,$$

or by

$$x = qrsx',\quad y = rspy',\quad z = spqz',\quad t = pqrt'.$$

Next we may suppose that a, b, c, d have no common factor, and hence also that no three of a, b, c, d have a common factor. For if

$$a = \omega a',\quad b = \omega b',\quad c = \omega c',\quad d \not\equiv 0 \pmod{\omega},$$

where ω is a prime, then $t \equiv 0 \pmod{\omega}$ or $t = \omega t'$, and (1) becomes

$$a'x^2 + b'y^2 + c'z^2 + \omega dt'^2 = 0, \tag{1 . 1}$$

and now ω is not a common factor of three of the coefficients. Similarly for the other common factors of a, b, c, etc. Only a finite number of equations such as (1 . 1) can arise since $a'b'c'\omega d = abcd/\omega^2 < abcd$.

Clearly we may suppose that the highest common factor of x, y, z, t is 1, written as $[x, y, z, t] = 1$, and so no three of x, y, z, t have a common factor since $a, b, \ldots$ have no squared factors. Finally we need consider only those solutions for which $[x, y, c, d] = 1$ or 2, together with the five similar restrictions obtained by permuting the letters. For if

$$x = \omega x',\quad y = \omega y',\quad c = \omega c',\quad d = \omega d',$$

where ω is an odd prime, (1) becomes

$$\omega ax'^2 + \omega by'^2 + c'z^2 + d't^2 = 0, \tag{1. 2}$$

where the coefficients still have no squared factors > 1 and ω is no longer a divisor of any two of the variables and also of the coefficients of the two remaining variables. Since

[1]) A. Meyer, Über die Kriterien für die Auflösbarkeit der Gleichung $ax^2 + by^2 + cz^2 + du^2 = 0$ in ganzen Zahlen, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich **29** (1884), 209—220.

$\omega a \omega b c' d' = abcd$, only a finite number of equations (1 . 2) can arise.

Write $[a, b]$ for the positive highest common factor of a and b and put

$$a = [a, b][a, c][a, d]\alpha, \quad b = [b, a][b, c][b, d]\beta, \quad c = [c, a][c, b][c, d]\gamma,$$
$$d = [d, a][d, b][d, c]\delta.$$

Then Meyer's criterion is that integer solutions of (1), really restricted as above, but not pointed out by him, exist if, and only if,

I a, b, c, d are not all of the same sign,

II $-[a, c][a, d][b, c][b, d]\gamma\delta$ is a quadratic residue of $[a, b]$, or what is readily seen to be equivalent, $-cd$ is a quadratic residue of $[a, b]$; together with five corresponding conditions derived by permuting the letters.

It is convenient to write pRq in place of the phrase „p is a quadratic residue of q". This phrase signifies that the congruence $\zeta^2 \equiv p \pmod q$ can be satisfied by integer values of ζ.

III Either III_1, $abcd \equiv 2, 3, 5, 6, 7 \pmod 8$,
or III_2, $abcd \equiv 1 \pmod 8$, $a + b + c + d \equiv 0 \pmod 8$,
or if $abcd \equiv 4 \pmod 8$ so that two and two only of a, b, c, d are even, say a, b, then

$$\mathrm{III}_3, \quad \frac{1}{4} abcd \equiv 3, 5, 7 \pmod 8,$$

$$\text{or} \quad \mathrm{III}_4, \quad \frac{1}{4} abcd \equiv 1 \pmod 8, \quad \frac{1}{2} a + \frac{1}{2} b + c + d \equiv \frac{c^2 d^2 - 1}{2} \pmod 8.$$

I remark that III_2 can be replaced by the exclusion of the cases typified by

$$a \equiv b \pmod 8, \quad c \equiv d \pmod 8, \quad a \equiv c \pmod 4.$$

For if $abcd \equiv 1 \pmod 8$, either the residues of $a, b, c, d \pmod 8$ are all different, i. e. are 1, 3, 5, 7 in some order, and then their sum is divisible by 8; or at least two have the same residue (mod 8), say a and b, and consequently $c \equiv d \pmod 8$, and then their sum is divisible by 8 only when $a \equiv -c \pmod 4$.

So for III_4, we need only exclude the three cases

$$\frac{1}{2} a \equiv \frac{3}{2} b \pmod 8, \quad c \equiv 3d \pmod 8;$$

$$\frac{1}{2} a \equiv \frac{1}{2} b \pmod 8, \quad c \equiv d \pmod 8, \quad \frac{1}{2} a \equiv c \pmod 4;$$

$$\frac{1}{2} a \equiv \frac{5}{2} b \pmod 8, \quad c \equiv 5d \pmod 8, \quad \frac{1}{2} a \equiv -c \pmod 4.$$

Firstly, the conditions I, II, III are necessary. Suppose for example that ω is an odd prime factor of $[c, d]$. Take (1) as a congruence mod ω, so that

$$ax^2 + by^2 \equiv 0 \pmod \omega.$$

As neither x nor y can be divisible by ω unless both were, $-abR\omega$ and this agrees with II.

The condition III means only that the congruence

$$ax^2 + by^2 + cz^2 + dt^2 \equiv 0 \pmod{2^n} \tag{2}$$

for any n, can be solved in integres x, y, z, t no three of which have the common factor 2. Clearly if (1) has integer solutions, (2) must be solvable. It is a simple matter [2]) to show that (2) will be solvable for all n if it is solvable for $n = 3$ when at most one of a, b, c, d

[2]) cf. Sommer, Vorlesungen über Zahlentheorie (1907), 133.

is even; or if it is solvable for $n = 4$ when two of a, b, c, d, say a, b, are even, so that z, t may also be both even.

Hence II, III are really identical with the condition that the congruence

(3) $ax^2 + by^2 + cz^2 + dt^2 \equiv 0 \pmod{8[a, b][b, c][c, a][a, d][b, d][c, d] = M}$

should be solvable in integers such that $[x, y, [c, d]] = 1$ or 2 and similarly for the others. The congruence (3) is always possible [3]) if the modulus M is replaced by any number prime to M.

The discussion of (2) will be facilitated by recalling that if f, g, h are odd numbers and x, y, z are integers no two of which are even, then the congruence

(4) $$fx^2 + gy^2 + hz^2 \equiv 0 \pmod{8}$$

is impossible if and only if

$$f \equiv g \equiv h \pmod{4}.$$

The congruence

(5) $$2fx^2 + gy^2 + hz^2 \equiv 0 \pmod{8}$$

is impossible if and only if

$$\frac{g^2h^2 - 1}{8} + \frac{gh + 1}{2} \cdot \frac{fh + 1}{2} \equiv 1 \pmod{2}.$$

These are easily verified on considering the different cases arising according to the residues of $f, g, h \pmod 8$, and are given in a slightly different form by Sommer (l. c., p. 134—135).

It is now sufficient, and easy, to verify that (2) is impossible in the cases I have excluded, e. g. if a and c are odd,

$$a(x^2 + y^2) + c(z^2 + t^2) \equiv 0 \pmod{8}$$

is not solvable when $a \equiv c \pmod 4$. Again if a, b are each double an odd number, and c, d are odd,

$$a(x^2 + 5y^2) + c(z^2 + 5t^2) \equiv 0 \pmod{16}$$

is impossible if $\frac{1}{2}a \equiv -c \pmod 4$. If $\frac{1}{2}a \equiv c \pmod 4$, a solution is obvious with x, z, t odd and $y \equiv 0 \pmod 4$.

§ 2. Meyer's published proof, and also the account of it given by Bachmann [4]), are restricted to the case when a, b, c, d are all odd. It is based on the arithmetical theory of ternary quadratic forms. The theorems involved require for their proof a number of others demanding considerable attention to many details and not lying on the surface, e. g. two primitive indefinite ternary quadratics of the order (Ω, Δ) where Ω, Δ are odd and prime to each other, are equivalent if and only if they belong to the same genus.

I show here that Meyer's results, including the cases when *abcd* is not odd, can be proved easily with a minimum of calculation and theory by using Legendre's classical theorem on the indeterminate equation

(6) $$Ax^2 + By^2 + Cz^2 = 0.$$

Meyer gives, without proof [5]), two further theorems. Let f_n be a primitive, indefinite quadratic form in the n variables $x_r, r = 1, \ldots, n$, and with non-zero discriminant.

---

[3]) cf. Sommer, 130.

[4]) Bachmann, Die Arithmetik der quadratischen Formen (1898), 233—266. Meyer's results are discussed in p. 259—266. The book is the first part of the fourth volume of Bachmann's Zahlentheorie.

[5]) Meyer, l. c. 218—222.

He states the necessary and sufficient conditions that $f_4 = 0$ should be solvable in integers not all zero.

By expressing f_4 as a sum of four linear squares, and noting the details involved in justifying the assumptions made in (1) about the common factors that might occur in the constants and variables, it is clear that

$$f_4(x_1, x_2, x_3, x_4) = 0 \tag{4}$$

is solvable if and only if the congruence

$$f_4(x_1, x_2, x_3, x_4) \equiv 0 \pmod{\omega^n} \tag{8}$$

is solvable for every prime ω and every n by integers not all divisible by ω. In fact, only a finite number of values of ω are required, namely 2 and possibly the odd divisors of the discriminant of the form f_4. Also we need only take one value of n ($\geqq 0$), which can be assigned by utilising the canonical form of f_4 expressed by means of linear squares and which also gives the explicit conditions.

He states next that $f_5 = 0$ is always solvable, and I prove this also very simply.

All his results are particular cases of general theorems given later by Minkowski [6]) who employs the arithmetical theory of the general quadratic form in n variables. Bachmann [7]) gives a brief outline of Minkowski's methods.

Finally there is a fairly recent paper by Hasse [8]) who deals with the general equation $f_n = 0$. He uses the mechanism of Hensel's p-adic numbers, but the foundations of my methods are essentially the same as his. Naturally the presentation and details are different as my objects are not altogether the same as those of his paper. It must be mentioned though that his ideas have led him to further very important developments [9]) upon the equivalence of quadratic forms and the representation of numbers by them not only for the field of the rational numbers but also for that of the general algebraic number.

§ 3. The sufficiency of the conditions I, II, III is deduced from Legendre's [10]) theorem. If A, B, C are integers not all of the same sign, and none is zero nor have a squared factor, and no two have a common factor, then integer solutions of

$$Ax^2 + By^2 + Cz^2 = 0 \tag{6}$$

exist if and only if

$$-BC\,R\,A,\ -CA\,R\,B,\ -AB\,R\,C.$$

This can be put in a slightly different form more useful for our purpose by isolating a positive factor λ of C where λ is a prime number (including 1) or twice a prime number. The condition $-AB\,R\,C$ is replaced by the condition $-AB\,R\,(C/\lambda)$ and by the possibility of the congruence

$$Ax^2 + By^2 + Cz^2 \equiv 0 \pmod 8 \tag{9}$$

in integers, no two of which are even.

In fact, a necessary condition for the solvability of (6) is the possibility of the congruence [with of course $[x, y, z] = 1$]

---

[6]) Minkowski, Über die Bedingungen, unter welchen zwei quadratische Formen mit rationalen Koeffizienten ineinander rational transformiert werden können, Journal für die reine und angewandte Mathematik **106** (1890), 5—26, or Gesammelte Abhandlungen **1** (1911), 219—239.

[7]) Bachmann, l. c. 551—553.

[8]) Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Journal für die reine und angewandte Mathematik **152** (1923), 129—148.

[9]) Ibid., 205—224, and **153** (1923), 12—43 und 113—130.

[10]) Bachmann, l. c. 202.

$$(10) \qquad Ax^2 + By^2 + Cz^2 \equiv 0 \pmod{4ABC}.$$

Not only is this sufficient for the existence of integer solutions of (6), but the factor 4 in the modulus is redundant, i. e. if (10) can be satisfied mod ABC it can also be satisfied mod $4ABC$. More generally if (10) is possible mod $4ABC/\lambda$, it is also possible mod $4ABC$ as is known [11]) from the theory of Hilbert's symbol of the norm residue.

This result is really equivalent to the general law of quadratic reciprocity, and can also be deduced directly. For put $C = \lambda C'$, so that the possibilty of (6) means that

$$-BC'\lambda R A, \quad -AC'\lambda R B, \quad -AB R C', \quad -AB R \lambda.$$

Hence this defines the quadratic characters of $-\lambda$ with respect to A and B and of $-AB$ with respect to λ. The law of quadratic reciprocity shows that a condition of consistency may be required, since if P and Q are two odd coprime numbers of which the first is positive,

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}, \qquad \left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}, \qquad \left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}},$$

using the Legendre-Jacobi symbol. This condition defines the residue of λ mod 4 or 8, and can only be the same as that for the possibility of the congruence (9).

As an illustration suppose

$$ABC \equiv 1 \pmod 2, \qquad A > 0, \qquad B > 0, \qquad C < 0.$$

Then $\left(\frac{\lambda}{A}\right) = \left(\frac{-BC'}{A}\right)$, $\left(\frac{\lambda}{B}\right) = \left(\frac{-AC'}{B}\right)$, $\left(\frac{-AB}{\lambda}\right) = 1$, $\left(\frac{-AB}{C'}\right) = 1$.

The first two give

$$\left(\frac{\lambda}{AB}\right) = \left(\frac{-B}{A}\right)\left(\frac{-A}{B}\right)\left(\frac{C'}{AB}\right).$$

The last two give

$$\left(\frac{\lambda}{AB}\right) = (-1)^{\frac{\lambda-1}{2}\cdot\frac{AB+1}{2}}, \qquad \left(\frac{C'}{AB}\right) = -(-1)^{\frac{C'-1}{2}\cdot\frac{AB+1}{2}},$$

the latter because $C' < 0$.

Since

$$\left(\frac{-B}{A}\right)\left(\frac{-A}{B}\right) = (-1)^{\frac{A-1}{2}\cdot\frac{B-1}{2}+\frac{A-1}{2}+\frac{B-1}{2}},$$

the condition of consistency becomes

$$(11) \qquad \frac{\lambda-1}{2}\cdot\frac{AB+1}{2} \equiv \frac{A-1}{2}\cdot\frac{B-1}{2} + \frac{A-1}{2} + \frac{B-1}{2} + \frac{AB+1}{2}\cdot\frac{C'-1}{2} + 1 \pmod 2.$$

If $AB \equiv 3 \pmod 4$, i. e. $A \equiv 1, B \equiv 3$ or $A \equiv 3, B \equiv 1 \pmod 4$, (11) is an identity in λ and (9) is solvable for all λ.

If $A \equiv B \equiv 1 \pmod 4$,

(11) becomes

$$\frac{\lambda-1}{2} \equiv \frac{C'+1}{2} \pmod 2,$$

$$\lambda \equiv C' + 2 \pmod 4,$$

and (9) is solvable only for this odd value of λ as then $\lambda C' \not\equiv 1 \pmod 4$.

If $A \equiv B \equiv 3 \pmod 4$,

(11) becomes

---

[11]) Sommer, l. c. 145.

$$\frac{\lambda - 1}{2} \equiv \frac{C' - 1}{2} \pmod 2,$$

$$\lambda \equiv C' \pmod 4,$$

and (9) is solvable only for this odd value of λ as then $\lambda C' \not\equiv 3 \pmod 4$.

It may be remarked that [11a]) an infinity of solutions of (6) exist with z prime to a given odd number M. For if ξ, η, ζ are one solution, it is easily verified that

$$x = C\xi + 2\lambda C\zeta - A\xi\lambda^2, \quad y = C\eta + A\eta\lambda^2,$$
$$z = -C\zeta + 2A\xi\lambda + A\zeta\lambda^2,$$

where λ is arbitrary, is another. Now $[C\zeta, A\xi, A\zeta] = 1$, if $[\xi, \eta, \zeta] = 1$, and so integer values can be assigned to λ for which z is prime to M.

Finally it might be noted that on considering the assumptions made for A, B, C integer values can be in (6) and the method of reducing the equation

$$A'x^2 + B'y^2 + C'z^2 = 0$$

to such a form (cf. the procedure for (1)), the following theorem becomes clear. If $f(x, y, z)$ is an indefinite ternary quadratic form, the equation

$$f(x, y, z) = 0$$

admits of integer solutions not all zero if and only if the congruence

$$f(x, y, z) \equiv 0 \pmod{\omega^n}$$

is possible for all primes ω and indices n with $[x, y, z]$ prime to ω. Naturally the only values of ω that matter are 2 and the divisors of the discriminant of $f(x, y, z)$. Also for given ω, it suffices to take only one value of n easily assigned from the canonical form of $f(x, y, z)$.

This result is of course included in that [12]) of H. J. S. Smith upon such equations.

§ 4. I now prove that a number $\lambda > |abcd|$ which is either a prime or twice a prime can be found such that the equations

$$aX^2 + bY^2 = [a, b][c, d]\lambda V^2, \tag{12}$$

$$cZ^2 + dT^2 = -[a, b][c, d]\lambda U^2, \tag{13}$$

each have an infinity of integer solutions in X, Y, V and Z, T, U respectively, where

$$[X, Y, V] = 1 = [Z, T, U].$$

As remarked, it may be supposed that U has at most a common factor 2 with any one of the six numbers $[a, b]$ etc. and similarly for V.

Then a solution of (1) is given by

$$x = XU, \quad y = YU, \quad z = ZV, \quad t = TV.$$

For clearly

$$ax^2 + by^2 + cz^2 + dt^2 = 0,$$

and it is easily verified that the six conditions such as

$$[x, y, [c, d]] = 1 \text{ or } 2, \text{ etc.},$$

are satisfied since a, b, c, d are free from squared factors. Thus x is prime to $[c, d]$ since a common factor of X and $[c, d]$ would occur in Y and hence in V.

Now (12) is solvable if and only if

[11a]) This is a particular case of a theorem given by Goldscheider, Das Reziprozitätsgesetz der achten Potenzreste, Prog. Berlin (1889), S. 8.

[12]) cf. Bachmann, l. c. 231—233.

$$\frac{a}{[a,b]}[c,d]\,\lambda R\,\frac{b}{[a,b]}, \tag{12. 1}$$

$$\frac{b}{[a,b]}[c,d]\,\lambda R\,\frac{a}{[a,b]}, \tag{12. 2}$$

$$\frac{-ab}{[a,b]^2}R[c,d], \tag{12. 3}$$

and

$$aX^2 + bY^2 \equiv \mu V^2 \pmod 8, \tag{12. 4}$$

where $\mu = [a,b][c,d]\lambda$, is a solvable congruence.

But (12. 3) is given in II and (12. 1), (12. 2) merely define the quadratic characters of λ with respect to the odd prime factors of $ab/[a,b]^2$.

Similary (13) is solvable if and only if

$$\frac{-c}{[c,d]}[a,b]\,\lambda R\,\frac{d}{[c,d]}, \tag{13. 1}$$

$$\frac{-d}{[c,d]}[a,b]\,\lambda R\,\frac{c}{[c,d]}, \tag{13. 2}$$

$$\frac{-cd}{[c,d]^2}R[a,b], \tag{13. 3}$$

and

$$cZ^2 + dT^2 \equiv -\mu U^2 \pmod 8 \tag{13. 4}$$

is a solvable congruence. Here (13. 3) ist included in II and (13. 1), (13. 2) define the quadratic characters of λ with respect to the odd prime factors of $cd/[c,d]^2$. Hence a condition of consistency will arise from the common odd prime factors of

$$ab/[a,b]^2,\ cd/[c,d]^2,$$

i. e. those occurring in any of

$$[a,c],[a,d],[b,c],[b,d].$$

But (12. 1), (13. 1) show that any odd prime factor of $[b,d]$, say, must be a quadratic residue of the product of their left hand terms, i. e. of $-ac$ and so the condition of consistency is included in II.

The assigning of the quadratic characters of λ restricts it to an arithmetical progression which by Dirichlet's theorem will clearly contain an infinity of primes and also of numbers which are double a prime.

§ 5. It still remains to be shown that a number $\lambda \not\equiv 0 \pmod 4$ exists such that each of the congruences (12. 4), (13. 4), or for that matter a particular pair obtained from them by any permutation of the four letters a, b, c, d, is solvable.

Suppose first a, b, c, d are all odd. Then (12. 4) is possible for any odd number λ unless

$$a \equiv b \equiv -\mu \pmod 4,$$

and (13. 4) is possible for any odd number λ unless

$$c \equiv d \equiv \mu \pmod 4.$$

Hence (12. 4), (13. 4) are both solvable except perhaps when

$$a \equiv b \equiv c \equiv d \pmod 4.$$

We then try if an even number suffices for λ. Put $\mu = 2\nu$. Then (12. 4) is solvable for any odd ν except when

$$(14.1) \qquad \frac{a^2b^2-1}{8} + \frac{ab+1}{2} \cdot \frac{av-1}{2} \equiv 1 \pmod 2,$$

and (13. 4) also except when

$$(14.2) \qquad \frac{c^2d^2-1}{8} + \frac{cd+1}{2} \frac{cv+1}{2} \equiv 1 \pmod 2.$$

At least two of the numbers, a, b, c, d are congruent mod 8, say a, b. Then (14. 1) becomes

$$\frac{av-1}{2} \equiv 1 \pmod 2, \qquad v \equiv 3a \pmod 4.$$

If and only if this value of v satisfies (14. 2), can (12. 4), (13. 4) both be solvable for the even λ. (We take therein $v \equiv 3a + 2 \pmod 4$. But as $3ac + 1 \equiv 0 \pmod 4$, this means

$$\frac{c^2d^2-1}{8} \equiv 1 \pmod 2, \qquad cd \equiv 5 \pmod 8.$$

Hence (12. 4), (13. 4) are not solvable for the even λ when

$$a \equiv b \pmod 8, \quad c \equiv d \pmod 8, \quad a \equiv c \pmod 4.$$

We have already seen that (2) is impossible in this case.

Next suppose only one of a, b, c, d is even, say $a = 2\alpha$, is twice an odd number. Then (13. 4) is solvable for any odd λ unless

$$(15.1) \qquad c \equiv d \equiv -\mu \pmod 4,$$

and (12. 4) also unless

$$(15.2) \qquad \frac{b^2\mu^2-1}{8} + \frac{b\mu-1}{2} \cdot \frac{\alpha b+1}{2} \equiv 1 \pmod 2.$$

The change of μ into $\mu + 4$ alters the residue of the left hand side of (15. 2) mod 2. Hence (12. 4), (13. 4) are both solvable for the same μ on taking one of

$$-\mu \equiv c + 2, \quad c - 2 \pmod 8.$$

Take finally the case when a and b are each double an odd number. Put

$$a = 2\alpha, \quad b = 2\beta, \quad c = \gamma, \quad d = \delta.$$

We can take instead of the congruences (12. 4), (13. 4) the pair

$$(16.1) \qquad 2\alpha x^2 + \gamma z^2 \equiv vV^2 \pmod{16},$$
$$(16.2) \qquad 2\beta y^2 + \delta t^2 \equiv -vU^2 \pmod{16},$$

where $[x, z, V] = [y, t, U] = 1$, $v \not\equiv 0 \pmod 4$, and mod 16 can be replaced by mod 8 if the corresponding z or t is odd. If v is even, z and t are even and then x, y are odd. If v is odd, z and t are odd and x, y are even. This means that the congruences (16. 1), (16. 2) can be replaced by the pair obtained on interchanging α, γ and β, δ.

Now (16. 1) is solvable for any odd v except when

$$(17.1) \qquad \frac{v^2\gamma^2-1}{8} + \frac{v\gamma-1}{2} \cdot \frac{\alpha\gamma+1}{2} \equiv 1 \pmod 2$$

and (16. 2) also except when

$$(17.2) \qquad \frac{v^2\delta^2-1}{8} + \frac{v\delta+1}{2} \cdot \frac{\beta\delta+1}{2} \equiv 1 \pmod 2.$$

Clearly (17. 1) is not satisfied by $v \equiv \gamma \pmod 8$ as $\gamma^2 \equiv 1 \pmod 8$, nor by $v \equiv \gamma + 2\alpha \pmod 8$, as then the left hand side of (17. 1) is congruent mod 2 to

$$\frac{1}{2}\alpha(\alpha+\gamma)\gamma^2 + \frac{1}{2}\alpha\gamma(\alpha\gamma+1) \equiv \frac{1+\alpha\gamma}{2} + \frac{1+\alpha\gamma}{2} \equiv 0.$$

Hence (16. 1), (16. 2) are both solvable if a value of ν exists such that

$$\nu \equiv \gamma \text{ or } \gamma + 2\alpha \pmod 8,$$

and also
$$-\nu \equiv \delta \text{ or } \delta + 2\beta \pmod 8.$$

These are consistent if

(18. 1) $\gamma \equiv -\delta, -\delta - 2\alpha, -\delta - 2\beta$, or $-\delta - 2\alpha - 2\beta \pmod 8$.

By symmetry (16. 1), (16. 2) are also solvable if

(18. 2) $\alpha \equiv -\beta, -\beta - 2\gamma, -\beta - 2\delta$, or $-\beta - 2\gamma - 2\delta \pmod 8$.

To discuss what restrictions are really involved, we note either

$$\alpha \equiv -\beta \pmod 4 \text{ or } \alpha \equiv \beta \pmod 4.$$

For the first, (18. 1) becomes

$$\gamma \equiv -\delta, -\delta - 2\alpha, \text{ or } -\delta + 2\alpha \pmod 8,$$

leaving still open

$$\gamma \equiv -\delta + 4 \pmod 8.$$

As $\alpha \equiv -\beta \pmod 8$ is included in (18. 2), we may also suppose

$$\alpha \equiv -\beta + 4 \pmod 8.$$

These mean

$$\alpha \equiv 3\beta \pmod 8, \ \gamma \equiv 3\delta \pmod 8,$$

and then

(19) $$2\alpha x^2 + 2\beta y^2 + \gamma z^2 + \delta t^2 \equiv 0 \pmod{16}$$

is impossible as already noted.

Next suppose $\alpha \equiv \beta \pmod 4$ so that (18. 1) becomes

$$\gamma \equiv -\delta, -\delta - 2\alpha, -\delta - 4\alpha \pmod 8,$$

leaving still for discussion

(19. 1) $$\gamma \equiv -\delta + 2\alpha \pmod 8, \ \alpha \equiv \beta \pmod 4.$$

By symmetry we may also suppose

(19. 2) $$\alpha \equiv -\beta + 2\gamma \pmod 8, \ \gamma \equiv \delta \pmod 4.$$

We then consider instead of (16. 1), (16. 2) the pair

(20. 1) $$\alpha x^2 + \beta y^2 \equiv \nu V^2 \pmod 8,$$

(20. 2) $$\gamma z^2 + \delta t^2 \equiv -2\nu U^2 \pmod 8.$$

Now (20. 1) is possible for any odd ν unless

(21. 1) $$\alpha \equiv \beta \equiv -\nu \pmod 4$$

and (20. 2) also unless

(21. 2) $$\frac{\gamma^2\delta^2 - 1}{8} + \frac{\gamma\delta + 1}{2} \cdot \frac{\nu\gamma + 1}{2} \equiv 1 \pmod 2.$$

Hence (20. 1), (20. 2) are both possible if and only if (taking $\alpha \equiv \beta \pmod 4$ of course) (21. 1), (21. 2) are consistent in ν, i. e.

(22) $$\frac{\gamma^2\delta^2 - 1}{8} + \frac{\gamma\delta + 1}{2} \cdot \frac{\alpha\gamma - 1}{2} \equiv 1 \pmod 2,$$

and then $\nu \equiv \alpha \pmod 4$ makes (20. 1), (20. 2) both solvable.

The case given by (19. 1), (19. 2) can be divided into four others according to the residues of α/β and $\gamma/\delta \pmod 8$.

If $\alpha \equiv \beta \pmod 8$, $\gamma \equiv \delta \pmod 8$, then $\alpha \equiv \gamma \pmod 4$, (22) is not satisfied, and we have already seen that (19) is now impossible.

If $\alpha \equiv 5\beta \pmod 8$, $\gamma \equiv 5\delta \pmod 8$, then from (19. 1), $\alpha \equiv -\gamma \pmod 4$, (22) is not satisfied and again (19) is impossible.

Finally we may take the two cases typified by

$$\alpha \equiv 5\beta \pmod 8, \quad \gamma \equiv \delta \pmod 8,$$

and so from (19. 1),

$$\alpha \equiv \gamma \pmod 4.$$

But this does not satisfy (19. 2), as $2\gamma \equiv 2\alpha \pmod 8$ giving $\alpha \equiv \beta \pmod 8$. Hence (16. 1), (16. 2) are now solvable.

This completes the proof.

§ 6. Meyer's paper [13]) includes a second part wherein he deals with the equation

$$ax^2 + by^2 + cz^2 + du^2 + ev^2 = 0 \tag{23}$$

where of course the given integers a, b, c, d, e do not all have the same sign. He shows there is no loss of generality in assuming that no three of a, b, c, d, e have a common factor. Suppose also that they are free from squared factors. He proves again by the theory of the ternary quadratic that (23) has integer solutions when a, b, c, d, e are all odd, and an account is given by Bachmann [14]). Meyer states that the result also holds for even values of a, etc. (we may suppose at most two of them are even, perhaps d, e).

These results are immediate deductions from (1). For put $u = pt$, $v = qt$ where p and q are integers to be assigned and t is a new variable.
The equation (23) becomes

$$ax^2 + by^2 + cz^2 + (dp^2 + eq^2)t^2 = 0.$$

We may suppose p, q taken so that $dp^2 + eq^2$ is prime to abc since

$$[a, d, e] = [b, d, e] = [c, d, e] = 1.$$

The conditions II reduce to three such as $-a(dp^2 + eq^2)\, R[b, c]$, i. e. $dp^2 + eq^2$ and hence p, q have assigned quadratic characters mod $[a, b]\,[b, c]\,[c, a]$.

The conditions III can also be satisfied. For if a, b, c, d, e are all odd, we may assume $d \equiv e \pmod 4$. Take p, q both odd and then $dp^2 + eq^2 \equiv \pm 2 \pmod 8$. If d or d, e only are even, take p odd, $q \equiv 0 \pmod 4$, and again $dp^2 + eq^2 \equiv \pm 2 \pmod 8$.

Hence the conditions I, II, III can be satisfied and the result.

The result as to $f_5 = 0$ clearly follows on expressing f_5 linearly by means of five squares.

---

[13]) Meyer, l.c. 220—222.

[14]) Bachmann, l. c. 266—268.

Eingegangen 10. Mai 1930.

Über die Struktur reeller Kurven.

Von *Otto Haupt* in Erlangen.

Einleitung.

0,1. Die folgenden Bemerkungen betreffen die Frage nach der Struktur zunächst der ebenen Bogen, d. h. der eindeutigen stetigen Streckenbilder. „Frage nach der Struktur" soll hier heißen: Aufsuchung primitivster Bogentypen, aus denen sich (in höchstens abzählbarer Anzahl) jeder vorgelegte Bogen zusammensetzen läßt. Die nähere Festlegung des Begriffes „primitiv" wird sich im Verlaufe der Untersuchung ergeben.

Diese Frage nach der Struktur eines Bogens hat Herr Hjelmslev in einer fundamentalen Arbeit [1]) behandelt. Neben vielen anderen Sätzen beweist nämlich Herr Hjelmslev beispielsweise [2]), daß *jeder gewöhnliche, keine Strecken enthaltende Bogen von höchstens endlicher Ordnung darstellbar ist als Vereinigungsmenge von höchstens abzählbar unendlich vielen Konvexbogen und von deren Häufungspunkten.* (Ein Bogen heißt von „höchstens endlicher Ordnung", wenn er von jeder Geraden in höchstens endlich vielen Punkten getroffen wird: Genaueres hierüber in Nr. 1,2). Unter einem „*gewöhnlichen*" Bogen („arc ordinaire") ist dabei ein ebener einfacher Bogen (also ein ein-eindeutiges stetiges Streckenbild) zu verstehen, bei welchem in jedem Punkte nur eine einzige vordere sowohl als hintere orientierte Halbtangente existiert und beide zusammenfallen. Den Beweis führt Herr Hjelmslev, indem er zunächst zeigt, daß jeder gewöhnliche, nirgends konvexe Bogen, d. h. jeder gewöhnliche Bogen, welcher keinen konvexen Teilbogen besitzt, von unendlicher Ordnung ist [3]). Da nun trivialerweise jeder (gewöhnliche) Bogen aus höchstens abzählbar vielen Strecken, konvexen und nirgends-konvexen Bogen aufgebaut werden kann, so ergibt sich aus dem Bewiesenen in der Tat der obige Satz über die gewöhnlichen Bogen endlicher Ordnung.

0,2. Durch die Feststellungen von Herrn Hjelmslev ist die Strukturfrage für den Fall der gewöhnlichen Bogen, insbesondere von höchstens endlicher Ordnung, bereits beantwortet. Es fragt sich nun, inwieweit die Beschränkung auf *gewöhnliche* Bogen für die Gültigkeit des Satzes notwendig ist. Ohne weiteres ist klar, daß der Satz allgemeiner für Bogen gilt, die sich ihrerseits als Vereinigung von (höchstens abzählbar vielen) gewöhnlichen Bogen darstellen lassen. Darüber hinaus hat aber Herr Rosenthal mit Hilfe seiner weitreichenden Sätze über die Singularitäten beliebiger reeller ebener Parameterkurven [4]) bewiesen, daß der Hjelmslevsche Satz auch noch gilt, wenn man Spitzen und mehrfache Punkte nicht ausschließt. Hingegen blieb unseres Wissens bisher dahingestellt,

[1]) Hjelmslev, J., Contribution à la géométrie infinitésimale de la courbe réelle. Oversigt over det kgl. Danske Videnskabernes selskabs Forhandlinger 1911, Seite 433 ff.

[2]) siehe [1]) a. a. O., Seite 482, Théorème 25.

[3]) siehe [1]) a. a. O., Seite 481, Théorème 24.

[4]) Rosenthal, A., Über die Singularitäten der reellen ebenen Kurven. Math. Ann. **73** (1913), Nr. 39.

ob auch hinsichtlich der Ecken keinerlei Einschränkungen nötig sind. Daß in der Tat keine solche Einschränkung nötig ist, daß also der Hjelmslevsche Satz für beliebige ebene Parameterbogen von höchstens endlicher Ordnung ohne Strecken gilt, wird sich im folgenden zeigen. Und zwar wird der so erweiterte Hjelmslevsche Satz seinerseits sich wiederum als spezielle Folgerung ergeben aus einer *Kennzeichnung derjenigen ebenen Bogen, welche sich lediglich aus Konvexbogen aufbauen lassen* (vgl. Nr. 0,5).

0,3. Bei unserem Beweise wird ein anderer Weg eingeschlagen als bei den Herren Hjelmslev und Rosenthal. Das wesentliche Hilfsmittel ist für uns der Begriff der *Ordnung eines Punktes auf dem Bogen*[5]): Wir schreiben einem Punkt P auf dem Bogen $\mathfrak{B}$ die „Ordnung n" bzw. „endliche Ordnung" bzw. „unendliche Ordnung" zu, wenn beliebig kleine Umgebungen von P auf dem Bogen $\mathfrak{B}$ die Ordnung n bzw. endliche Ordnung bzw. unendliche Ordnung besitzen. Es handelt sich bei unserer Definition also um eine Definition vermittelst Umgebungsfolgen, die sich auf einen Punkt zusammenziehen, ein Verfahren, welches von Herrn Menger[6]) in seiner Allgemeinheit und unter Hervorhebung seiner methodischen Wichtigkeit formuliert worden ist.

Diese Begriffsbildung führt sogleich zu einer hinreichenden und notwendigen Bedingung dafür, daß ein ebener Bogen sich lediglich aus Konvexbogen aufbauen läßt. Da nämlich ein Konvexbogen nur Punkte 2. Ordnung enthält, so ist, wie sich zeigen läßt, ein ebener Bogen $\mathfrak{B}$ dann (und nur dann) mit Hilfe lediglich von Konvexbogen darstellbar, wenn auf $\mathfrak{B}$ die Punkte höherer als 2. Ordnung nirgends dicht liegen. Zum Beweise des Hjelmlevschen Satzes bzw. seiner oben angeführten Verallgemeinerung muß daher nur noch gezeigt werden, daß auf einem Bogen endlicher Ordnung die Punkte höherer als 2. Ordnung nirgends dicht liegen.

0,4. Der hiermit angedeutete einfache Gedankengang des Beweises wird in den nachstehenden Ausführungen allerdings nicht genau innegehalten; es geschieht das, um die einzelnen Grundgedanken deutlich von einander abzuheben. Hierüber möge schon an dieser Stelle noch einiges Nähere gesagt werden:

Die Definition des Punktes n-ter Ordnung ist durchaus nicht an die ebenen Kurven gebunden, überträgt sich vielmehr ohne weiteres auf *Kurven, Flächen usw. im projektiven Raume von drei und mehr Dimensionen.* Für alle diese Verallgemeinerungen lassen sich nun, wie aus den späteren einfachen Überlegungen zu entnehmen ist, gleichzeitig, also *allgemein*, *Aussagen* machen über die Verteilung der Punkte der einzelnen Ordnungen auf dem jeweils betrachteten Gebilde (Kurve, Fläche usw.) (vgl. auch die weitergehenden Andeutungen in Nr. 0,6). Die fragliche Verteilung ist nämlich stets eine derartige, daß das betrachtete Gebilde sich zerlegen läßt in höchstens abzählbar unendlich viele Teilgebilde (sogen. „primitive" Gebilde), deren jedes *nur Punkte gleicher Ordnung enthält und überdies selbst (im großen) eben diese Ordnung besitzt.* Unsere Begriffsbildung führt also ohne weiteres allgemein zu näheren Formulierungen und zu bestimmten Fragen bezüglich der Struktur der Bogen im Raum usw.

Diese allgemeinen Überlegungen sind dann zu ergänzen durch *spezielle Untersuchungen* über die Natur und Existenz der primitiven Gebilde in den einzelnen jeweils betrachteten Fällen (der ebenen Kurven bzw. der Raumkurven bzw. der Flächen usw.).

0,5. Entsprechend dem vorstehend (Nr. 0,4) entwickelten Gedankengang wird im folgenden zunächst (Nr. 2,1—2,7) der Beweis des erwähnten allgemeinen Zerlegungs-

[5]) Der hier benutzte Begriff der „Ordnung" eines Kurvenpunktes (vgl. Erlanger Ber. **60** (1928), S. 327) ist verschieden von demjenigen, welchen Herr Menger in seiner Theorie der Kurven verwendet (vgl. z. B. Menger, K., Grundzüge einer Theorie der Kurven, Math. Ann. **95** (1925), Seite 279; die „Ordnung" des betrachteten Punktes wird dort durch die Mächtigkeit der Begrenzungen beliebig kleiner Umgebungen definiert).

[6]) Menger, K., Bericht über die Dimensionstheorie, Jahresber. d. d. Math. Vereinig. **35** (1926), Seite 131.

satzes am Beispiel der ebenen Kurven durchgeführt, in einer Form, die ohne weiteres die Verallgemeinerung gestattet. Hingegen beschränkt sich die spezielle Untersuchung (Nr. 3,1) in der gegenwärtigen Arbeit durchaus auf die ebenen Kurven, da für andere Fälle noch keine abschließenden Ergebnisse vorliegen [7]).

Es ergibt sich für den Fall der ebenen Kurven, daß — vom Fall der Strecke abgesehen — primitive Bogen nur von 2. Ordnung oder von unendlicher Ordnung existieren. Daraus folgt dann ohne weiteres, *daß jeder Bogen sich aus abzählbar vielen Strecken, Konvexbogen und primitiven Bogen unendlicher Ordnung zusammensetzt. Ferner folgt, daß ein keine Strecken enthaltender Bogen dann und nur dann aus lauter Konvexbogen sich aufbauen läßt, wenn die Punkte unendlich hoher Ordnung nirgends dicht liegen* [8]). Und darin ist der, in Nr. 0,2 erwähnte, erweiterte Hjelmslevsche Satz als Spezialfall enthalten.

0,6. Es mag an dieser Stelle noch andeutungsweise auf folgendes hingewiesen werden: Der in Nr. 0,4 erwähnte Zerlegungssatz ist wesentlich dadurch bedingt, daß die Umgebung eines Punktes von n-ter Ordnung keine Punkte höherer als n-ter Ordnung enthalten kann. Anders gesagt: Der Zerlegungssatz läßt sich in folgender Weise verallgemeinern: Es liege eine wohlgeordnete Menge E von Eigenschaften E_ν vor (ist e die Ordnungszahl von E, so bedeute also ν jede Ordnungszahl, die kleiner ist als e); jedes E_ν schließe alle übrigen aus. Ferner besitze z. B. jeder Bogen $\mathfrak{B}$ eine dieser Eigenschaften und kein Teilbogen von $\mathfrak{B}$ eine ranghöhere als $\mathfrak{B}$, d. h. wenn $\mathfrak{B}$ die Eigenschaft E_ν besitzt, so besitze jeder Teilbogen $\bar{\mathfrak{B}}$ von $\mathfrak{B}$ eine Eigenschaft E_μ, wobei $\mu \leqq \nu$. Betrachtet man alsdann die Gesamtheit aller Umgebungen eines Punktes P von $\mathfrak{B}$ auf dem Bogen $\mathfrak{B}$, so findet sich unter den E_ν, welche diesen Umgebungen zugehören, eine rangniedrigste, etwa E_ϱ. Man bezeichnet dann P als „Punkt ϱ-ter Art", und gelangt wiederum zum Zerlegungssatz.

1. Vorbemerkungen.

1,1. Soweit nicht ausdrücklich etwas anderes bemerkt wird, bedeutet im folgenden das Wort „Bogen" stets eine beschränkte Punktmenge in der euklidischen Ebene [9]), welche eindeutiges und stetiges Bild einer abgeschlossenen Strecke $[a, b]$ ist, welche also bezüglich etwa rechtwinkliger kartesischer Koordinaten x, y definiert ist als Menge $\mathfrak{B}$ der Punkte $P\{x, y\}$, für die

$$x = \varphi(t), \quad y = \psi(t), \quad a \leqq t \leqq b,$$

unter $\varphi(t)$, $\psi(t)$ reelle, eindeutige und stetige Funktionen des reellen Parameters t verstanden. Dabei soll *jedem Teilintervall von Parameterwerten mehr als ein Punkt* $P\{x, y\}$ *von* $\mathfrak{B}$ entsprechen [10]).

Den Fall, daß der Bogen $\mathfrak{B}$ Strecken als Teilbogen enthält, können wir für unsere Zwecke ausschließen (vgl. Nr. 2,1).

---

[7]) Immerhin kann man den in Nr. 3,1 bewiesenen Satz z. B. für den Raum R_3 von drei Dimensionen verallgemeinern, wenigstens dann, wenn man sich auf Klassen von Bogen beschränkt, die gewisse Differenzierbarkeitseigenschaften besitzen, Es zeigt sich nämlich, daß dann alle primitiven Bogen entweder von dritter oder von unendlicher Ordnung sind, falls von ebenen Bogen abgesehen wird. Entsprechendes gilt für mehr als drei Dimensionen.

[8]) Man vgl. übrigens hierzu die auf gewöhnliche Bogen bezüglichen Bemerkungen bei Hjelmslev [1]), a. a. O., Seite 481—483.

[9]) Diese Annahme bedeutet für unsere Untersuchung keine Beschränkung der Allgemeinheit und wird nur der bequemeren Darstellung wegen gemacht. Man kann natürlich gleich von vorneherein in der projektiven Ebene arbeiten. Vgl. z. B. [4]) a. a. O., Einleitung.

[10]) Ein „Intervall" sowie eine „Strecke" sollen stets (mindestens zwei) verschiedene Punkte enthalten.

Zum Unterschied von den „*Punkten*“ $P\{x, y\}$ des Bogens werden die zugehörigen Punkte der betr. Strecke $[a, b]$ bzw. die ihnen entsprechenden Parameterwerte t als die zu $P\{x, y\}$ zugehörigen „*Stellen*“ bezeichnet. Man bezeichnet ferner $P\{x, y\}$ als „*inneren*“ Punkt bzw. als „*Randpunkt*“ von $\mathfrak{B}$, je nachdem P als Bild einer Stelle im Innern bzw. am Rande der Strecke betrachtet wird.

Vielfache Punkte eines Bogens $\mathfrak{B}$, d. h. solche Punkte $P\{x, y\}$ auf $\mathfrak{B}$, welchen mehrere, verschiedene Stellen (d. h. Parameterwerte t) zugehören, werden im folgenden stets *mit* ihrer *Vielfachheit auf* $\mathfrak{B}$ *gezählt*, d. h. als soviel *verschiedene* Punkte, wie ihre Vielfachheit angibt (Vielfachheit auf $\mathfrak{B}$ = Anzahl (Kardinalzahl) der verschiedenen, zu P gehörigen Stellen in $[a, b]$).

Es sei $P\{x, y\}$ ein innerer Punkt von $\mathfrak{B}$, aufgefaßt als Bild der Stelle t_0. Unter einer *Umgebung* $\mathfrak{U}(P; \mathfrak{B})$ von P oder, besser, von t_0 auf $\mathfrak{B}$ verstehen wir einen *offenen* Teilbogen von $\mathfrak{B}$, welcher den *Stellen* $0 \leqq |t - t_0| < \delta$ entspricht ($\delta < 0$ hinlänglich klein, aber im übrigen beliebig gewählt). Das Bild von $0 \leqq |t - t_0| \leqq \delta$ soll als *abgeschlossene Umgebung* $\mathfrak{U}(P; \mathfrak{B})$ von P bzw. t_0 bezeichnet werden.

Anmerkung: Gehören die Punkte P bzw. Q zu den Stellen $t = p$ bzw. $t = q$, so heiße Q „*rechts*“ (bzw. „*links*“) von P auf $\mathfrak{B}$ gelegen, wenn $p < q$ (bzw. wenn $p > q$); dies soll also auch dann gelten, wenn P und Q in der Ebene zusammenfallen, wenn also $x(p) = x(q)$, $y(p) = y(q)$ ist. Demgemäß heißt dann z. B. das Bild von $p \leqq t < p + \delta$ ($\delta > 0$) eine *rechtsseitige Umgebung* von P auf $\mathfrak{B}$. Für die *Randpunkte* von $\mathfrak{B}$ (also für $t = a$ bzw. $t = b$) kommen nur solche einseitige Umgebungen in Frage, im Gegensatz zu den inneren Punkten von $\mathfrak{B}$.

Eine Gerade g heiße *Sekante n-ter Ordnung von* $\mathfrak{B}$ (oder „*an* $\mathfrak{B}$“ oder „*in* $\mathfrak{B}$“), wenn g mit $\mathfrak{B}$ genau n Punkte gemeinsam hat, wobei vielfache Punkte mit ihrer Vielfachheit gezählt werden ($n \geqq 1$). Hat g unendlich viele Punkte mit $\mathfrak{B}$ gemeinsam, so werde g als *Sekante unendlicher Ordnung* von $\mathfrak{B}$ bezeichnet. Zu diesen Definitionen ist ergänzend folgendes zu bemerken: Es sei P *innerer* Punkt von $\mathfrak{B}$ und es liege P auf einer Sekante g von $\mathfrak{B}$ so, daß eine passend gewählte (hinreichend kleine) $\mathfrak{U}(P; \mathfrak{B})$ „*ganz auf einer Seite von* $\mathfrak{B}$ *verläuft*“, d. h. daß alle Punkte einer $\mathfrak{U}(P; \mathfrak{B})$ in *einer* der beiden abgeschlossenen Halbebenen liegen, welche durch g definiert sind; in diesem Falle soll P als *Stützpunkt* von $\mathfrak{U}(P; \mathfrak{B})$ oder von $\mathfrak{B}$ auf g bezeichnet und soll übrigens — bei Bestimmung der Ordnung von g — (lediglich) mit seiner Vielfachheit gezählt werden. Enthält $\mathfrak{U}(P; \mathfrak{B})$ Punkte aus dem Innern einer *jeden* der beiden soeben genannten Halbebenen, so spricht man von einem *Schnittpunkt*.

Für unsere Zwecke ist später noch von Nutzen die folgende

Bemerkung: *Es sei g eine, beliebig vorgegebene, Sekante k-ter Ordnung an $\mathfrak{B}$ ($k \geqq 1$), auf welcher kein Randpunkt von $\mathfrak{B}$ liegt. Dann existieren Geradenbüschel von folgender Beschaffenheit: g gehört dem Büschel an; ferner sind alle, zu g hinreichend benachbarten Büschelgeraden $\bar{g}$ Sekanten an $\mathfrak{B}$ von mindestens k-ter Ordnung und zwar Sekanten, welche nur innere Punkte von $\mathfrak{B}$ enthalten.*

Diese Bemerkung ist zunächst richtig für den Fall, daß g nur (innere) *Schnitt*punkte enthält. Denn betrachten wir alsdann z. B. den Büschel von Parallelen zu g und beschränken uns auf Parallele $\bar{g}$, die zu g hinreichend benachbart sind, so können Randpunkte von $\mathfrak{B}$ niemals auf $\bar{g}$ liegen und ferner entspricht jedem Schnittpunkt auf g mindestens ein Schnittpunkt auf $\bar{g}$. Um auch den Fall zu erledigen, in welchem Stützpunkte auf g liegen, werde angenommen, daß die Sekante k-ter Ordnung g die Stützpunkte $P_1, \ldots, P_r$ bzw. $Q_1, \ldots, Q_s$ besitze, wobei $\mathfrak{U}(P_\varrho; \mathfrak{B})$, $\varrho = 1, \ldots, r$, sämtlich ganz auf der *einen* Seite von g liegen und $\mathfrak{U}(Q_\sigma; \mathfrak{B})$, $\sigma = 1, \ldots, s$, sämtlich ganz auf der anderen

Seite von g; ferner sei etwa $r \geqq s$, auch seien der Bequemlichkeit wegen die P_ϱ und Q_σ zunächst alle als nichtmehrfache Punkte angenommen. Verschiebt man jetzt g beliebig wenig parallel zu sich in diejenige Halbebene, welcher die $\mathfrak{U}(P_\varrho; \mathfrak{B})$ angehören, so entstehen aus dem Stützpunkt P_ϱ mindestens zwei Schnittpunkte, während die Punkte Q_σ „verlorengehen", d. h. keine in der Umgebung von Q_σ gelegenen Punkte von $\bar{g}$ liefern[11]). Wir erhalten so an Stelle der $r + s$ Punkte $P_1, \ldots, P_r$; $Q_1, \ldots, Q_s$ mindestens $2r$ Schnittpunkte, wobei $2r \geqq r + s$ ist. Bedenkt man noch, daß überdies jeder ursprünglich auf g vorhandene Schnittpunkt zu mindestens einem Schnittpunkt auf $\bar{g}$ führt, so ergibt sich der Beweis unserer Behauptung auch für den eben betrachteten Fall, daß Stützpunkte auf g existieren. Daß die Überlegungen auch für den Fall mehrfach zählender P_ϱ und Q_σ gelten, ist einleuchtend.

Zusatz: Besitzt $\mathfrak{B}$ keine Sekante von höherer als k-ter Ordnung, so sind die oben genannten, zu g benachbarten Sekanten $\bar{g}$ sämtlich von genau k-ter Ordnung und enthalten keine Stützpunkte, also nur Schnittpunkte.

In der Tat enthält $\bar{g}$ mindestens k Schnittpunkte, also auch keine weiteren Schnittpunkte oder gar Stützpunkte.

1,2. Die im Folgenden betrachteten Bogen sollen (wie in Nr. 1,1) keine Strecken als Teilbogen enthalten (vgl. Nr. 2,1). Ein *Bogen* $\mathfrak{B}$ heiße *von* (beschränkter) *n-ter Ordnung*, wenn $\mathfrak{B}$ nur Sekanten höchstens n-ter Ordnung besitzt, aber auch mindestens eine Sekante von genau n-ter Ordnung (*Maximalsekante*). Ferner heiße $\mathfrak{B}$ von *endlicher Ordnung*, wenn $\mathfrak{B}$ nur Sekanten endlicher Ordnungen besitzt, wenn aber die Ordnungen der Sekanten nicht beschränkt sind. Ist ein Bogen weder von beschränkter noch von endlicher Ordnung, so heiße er von „*unendlicher*" Ordnung.

Wir erklären schließlich die *Ordnung eines Punktes P auf* $\mathfrak{B}$. Man betrachte zu diesem Zwecke die Gesamtheit der Umgebungen[12]) von P auf $\mathfrak{B}$ und die Menge M ihrer Ordnungen. Da die Ordnung irgendeines Bogens nicht kleiner sein kann als die Ordnung eines beliebigen seiner Teilbogen, so enthält M entweder eine kleinste natürliche Zahl $n \geqq 2$ oder alle hinreichend kleinen Umgebungen sind von endlicher Ordnung oder alle sind von unendlicher Ordnung; je nachdem heißt P von n-ter bzw. von endlicher bzw. von unendlicher Ordnung auf $\mathfrak{B}$ (P ist alsdann, kurz gesagt, innerer (bzw. Rand-)Punkt von beliebig kleinen Bogen n-ter Ordnung usw.).

Durch Konstruktion von Beispielen beweist man die Existenz von Punkten beliebiger Ordnung.

1. *Zusatz*: Die Bogen bzw. Punkte unendlicher Ordnung kann man ihrerseits noch klassifizieren in solche von abzählbar unendlicher Ordnung und solche, deren Ordnung Kontinuumsmächtigkeit besitzt[13]). Im Interesse einer einfachen Formulierung unserer Sätze sehen wir aber von der hierdurch nahegelegten verfeinerten Einteilung der Punkte unendlicher Ordnung ab.

---

[11]) In der Tat: Ist etwa g durch $ax + by + c = 0$ gegeben und setzt man $G(t) = a\varphi(t) + b\psi(t) + c$, so zeigt sich, daß $G(t) - \bar{c}$ sowohl in $\mathfrak{U}^+(P_\varrho; \mathfrak{B})$ als in $\mathfrak{U}^-(P_\varrho; \mathfrak{B})$ das Vorzeichen wechselt, falls $\bar{c}$ eine reelle Zahl bedeutet, die absolut hinreichend klein und von passend gewähltem Vorzeichen ist. Wegen der Stetigkeit von $G(t)$ als Funktion von t folgt daraus die Existenz mindestens zweier verschiedenen, in $\mathfrak{U}(P_\varrho; \mathfrak{B})$ gelegenen Nullstellen von $G(t)$, in deren Nähe $G(t)$ verschiedene Vorzeichen besitzt w. z. z. w.

[12]) Und zwar einseitige Umgebungen nur im Falle eines Randpunktes P. Vgl. aber den 2. Zusatz in Nr. 1, 2.

[13]) Herr Rosenthal (vgl. [4]) a. a. O., Nr. 35) hat gezeigt, daß die Ordnung eines Bogens entweder beschränkt oder endlich oder abzählbar oder von der Mächtigkeit des Kontinuums ist und daß es andere Möglichkeiten nicht gibt. Die Behauptung folgt aus der Abgeschlossenheit der Menge aller Punkte (bzw. Stellen), welche einer Sekante und einem Bogen gemeinsam sind.

2. *Zusatz*: Nimmt man in den Definitionen des Punktes n-ter Ordnung usw. für innere Punkte statt der $\mathfrak{U}(P;\mathfrak{B})$ z. B. die rechtsseitigen Umgebungen $\mathfrak{U}^+(P;\mathfrak{B})$, so erhält man den Begriff des „*Punktes von rechtsseitiger n-ter Ordnung*“ usw.

3. *Zusatz*: Die Aussage des Zusatzes zu Nr. 1,1 bezieht sich auf Bogen k-ter Ordnung, Für den Fall eines *Bogens* $\mathfrak{B}$ *von endlicher Ordnung* kann man wenigstens folgendes behaupten: *Zu jeder Sekante g von* $\mathfrak{B}$ *läßt sich ein, g enthaltendes Büschel von parallelen Sekanten bestimmen von folgender Eigenschaft: Der Büschel enthält Sektoren, welche zu g beliebig benachbart*[14]) *sind und so beschaffen, daß alle Sekanten g* aus dem Sektor gleiche Ordnung besitzen und daß kein g* Stützpunkte aufweist.*

Die Behauptung folgt aus der Tatsache, daß Stützpunkte nur auf einer nirgends dichten Teilmenge von Büschelsekanten auftreten können, falls $\mathfrak{B}$ von endlicher Ordnung ist[15]); dabei heißt eine Menge von Büschelsekanten nirgends bzw. überall dicht, je nachdem die Menge ihrer Schnittpunkte mit einer festen, nicht zum Büschel gehörigen Geraden h nirgends dicht auf h liegt oder überall dicht. Auf Grund dieser Bemerkung kann man nun zunächst (aus dem, g enthaltenden Parallelenbüschel) einen Sektor auswählen, für welchen keine der zugehörigen Sekanten g^* Stützpunkte aufweist und welcher zu g beliebig benachbart ist. Und da die Ordnung m einer Sekante g^* bei Parallelverschiebung nur dadurch sich ändern kann, daß Randpunkte oder Stützpunkte passiert werden, so besitzen auch alle unsere g^* die gleiche Ordnung, falls nur der Sektor genügend schmal ist.

2. Allgemeiner Zerlegungssatz.

2,1. Bei Untersuchungen der von uns beabsichtigten Art kann man, wie dies von Anfang an geschehen ist (vgl. Nr. 1,1) *ohne Beschränkung der Allgemeinheit annehmen, daß der betrachtete Bogen* $\mathfrak{B}$ *keine Strecken*[10]) *enthalte.* In der Tat kann $\mathfrak{B}$ höchstens abzählbar unendlich viele (abgeschlossene) Strecken $\mathfrak{S}_\varrho$ enthalten und außer diesen noch höchstens abzählbar unendlich viele (abgeschlossene) Teilbogen $\mathfrak{B}_\nu$, in deren keinem eine Strecke enthalten ist. $\mathfrak{B}$ selber ist dann die Vereinigungsmenge aus den $\mathfrak{S}_\varrho$ und $\mathfrak{B}_\nu$ und aus den Häufungspunkten dieser Bogen. Und nur die $\mathfrak{B}_\nu$ sind noch weiter auf ihre Struktur hin zu untersuchen.

Im folgenden werden wir häufig Vereinigungsmengen aus endlich oder abzählbar unendlich vielen (abgeschlossenen) Bogen und aus den Häufungspunkten dieser Bogen zu betrachten haben; dabei ist dann immer angenommen, daß die Bogen zu je zweien höchstens Randstellen, d. h. keine inneren Stellen gemeinsam haben. Zur Abkürzung führen wir für solche Vereinigungsmengen die Bezeichnung „*abgeschlossene Summe*“ ein; handelt es sich nur um *endlich viele* Bogen, so sprechen wir auch kürzer von ihrer „*Summe*“.

2,2. Wir schicken noch einige naheliegende, aber für das Folgende nützliche Bemerkungen voraus:

Damit ein Bogen $\mathfrak{B}$ *Summe von endlich vielen Bogen sei, deren Ordnungen höchstens gleich n sind, ist notwendig und hinreichend, daß jeder Punkt von* $\mathfrak{B}$ *von höchstens n-ter*

---

[14]) Unter einem „Sektor“ ist natürlich ein im ursprünglichen Büschel enthaltenes Parallelenbüschel zu verstehen. Der Sektor S heißt „δ-benachbart“ zu g, wenn alle Parallelen aus S von g einen Abstand kleiner als δ besitzen ($\delta > 0$). „Beliebig benachbart“ heißt: δ beliebig klein.

[15]) Die Behauptung des Textes ist im wesentlichen gleichbedeutend mit einem Satze von Herrn Rosenthal. Vgl.[4]) a. a. O., Nr. 35. Der Beweis ergibt sich durch Konstruktion einer Sekante unendlicher Ordnung im Falle Stützpunkte auf einer überall dichten Sekantenmenge auftreten. In diesem Falle kann man nämlich schrittweise durch passende Parallelverschiebung stets neue Stützpunkte auf die Sekante werfen, während gleichzeitig die durch Auflösung (vgl. [11])) früher vorhandener Stützpunkte gewonnenen Schnittpunkte bzw. die zugehörigen Stellen sämtlich erhalten bleiben und nach unten beschränkte Abstände behalten (vgl. a. a. O.).

einseitiger Ordnung sei. Ist jeder Punkt von beschränkter Ordnung, so ist $\mathfrak{B}$ *Summe von endlich vielen Bogen, deren jeder eine beschränkte Ordnung besitzt.*

Dies folgt aus dem Heine-Borelschen Überdeckungssatz, weil (von Randpunkten abgesehen) jeder Punkt von höchstens n-ter (ev. einseitiger) Ordnung innerer Punkt eines Teilbogens von der gewünschten Eigenschaft ist.

Ein Bogen ist dann und nur dann von höchstens endlicher Ordnung, wenn er keine Punkte unendlicher Ordnung enthält (insbesondere also keine unendlich vielfachen Punkte).

Die Bedingung ist ersichtlich notwendig. Sie ist aber auch hinreichend: Denn jeder Bogen unendlicher Ordnung besitzt mindestens eine Sekante unendlicher Ordnung; auf dieser existiert aber mindestens ein Häufungspunkt H von Punkten bzw. Stellen des Bogens, und H ist daher ein Punkt unendlicher Ordnung.

2,3. *Die Menge der Punkte von mindestens k-ter Ordnung* ($k \geqq 2$) *ist auf* $\mathfrak{B}$ *abgeschlossen; ebenso die Menge der Punkte von mindestens endlicher (bzw. von unendlicher) Ordnung.* („Von mindestens k-ter [bzw. endlicher] Ordnung" soll heißen: Von einer Ordnung n ($n \geqq k$) oder von endlicher Ordnung oder von unendlicher Ordnung [bzw. von endlicher oder von unendlicher Ordnung]).

In der Tat: Ist P Häufungspunkt von Punkten z. B. mindestens k-ter Ordnung, so ist in jeder $\mathfrak{U}(P; \mathfrak{B})$ ein Teilbogen mindestens k-ter Ordnung enthalten, es ist also $\mathfrak{U}(P; \mathfrak{B})$ selber von mindestens k-ter Ordnung w. z. z. w.

Zusatz: Jeder Häufungspunkt von Punkten mindestens k-ter usw. Ordnung ist sogar von *einseitiger* mindestens k-ter usw. Ordnung.

2,4. Da die abgeschlossene Hülle einer auf $\mathfrak{B}$ überall dichten Punktmenge mit $\mathfrak{B}$ identisch ist, so folgt aus Nr. 2,3:

Dann (und nur dann) ist jeder Punkt auf $\mathfrak{B}$ *von mindestens k-ter (bzw. von mindestens endlicher bzw. von unendlicher) Ordnung, wenn die Punkte mindestens k-ter (bzw. mindestens endlicher bzw. unendlicher) Ordnung überall dicht auf* $\mathfrak{B}$ *liegen.*

2,5. *Liegen andererseits die Punkte mindestens* $(n+1)$*-ter (bzw. mindestens endlicher bzw. unendlicher) Ordnung nirgends dicht auf* $\mathfrak{B}$, *so ist* $\mathfrak{B}$ *darstellbar als abgeschlossene Summe von Bogen höchstens n-ter (bzw. je beschränkter bzw. je höchstens endlicher) Ordnung. Davon gilt auch die Umkehrung; d. h. wenn* $\mathfrak{B}$ *abgeschlossene Summe z. B. von Bogen höchstens n-ter Ordnung ist, dann liegen auf* $\mathfrak{B}$ *die Punkte mindestens* $(n+1)$*-ter Ordnung nirgends dicht oder — was das Gleiche — die Punkte höchstens n-ter Ordnung liegen überall dicht auf* $\mathfrak{B}$.

In der Tat: Sei A_{n+1} die (abgeschlossene) Menge aller Punkte von mindestens $(n+1)$-ter Ordnung auf $\mathfrak{B}$, ferner C_{n+1} das hinsichtlich $\mathfrak{B}$ gebildete (offene) Komplement von A_{n+1}. Wir denken uns die auf $\mathfrak{B}$ offene Menge C_{n+1} als Vereinigung von abzählbar vielen abgeschlossenen Teilbogen $\mathfrak{T}_\nu$ dargestellt, welche zu je zweien höchstens Randstellen gemeinsam haben; diese Darstellung ist ja immer möglich. Da C_{n+1} nur Punkte von höchstens n-ter Ordnung enthält, so ist jeder Teilbogen $\mathfrak{T}_\nu$ zufolge Nr. 2, 2 Summe von endlich vielen Bogen höchstens n-ter Ordnung. Beachtet man noch, daß C_{n+1} überall dicht auf $\mathfrak{B}$ und daß daher $\mathfrak{B}$ mit der abgeschlossenen Hülle von C_{n+1} identisch sein muß, so ergibt sich $\mathfrak{B}$ wirklich als abgeschlossene Summe von Bogen höchstens n-ter Ordnung. Durch die gleichen Schlüsse ergeben sich die übrigen Behauptungen, während die Umkehrung aus Nr. 2,4 zu entnehmen ist.

2,6. Die vorstehenden Bemerkungen führen jetzt leicht zur Zerlegung eines beliebigen Bogens in einfachste, in gewissem Sinne nicht weiter zerlegbare Bogen, die wir als „primitive Bogen" bezeichnen und des näheren definieren wollen, wie folgt: *Ein Bogen* $\mathfrak{P}$ *heiße primitiv* (von n-ter bzw. von endlicher bzw. von unendlicher Ordnung), *wenn*

alle seine Punkte von gleicher Ordnung sind (also von n-ter bzw. von endlicher bzw. von unendlicher Ordnung) *und wenn überdies der Bogen* $\mathfrak{P}$ *als Ganzes genau die gleiche Ordnung besitzt.* (Im Falle unendlicher Ordnung ist die zweite Forderung ersichtlich eine Folge der ersten.)

Zu dieser Definition muß bemerkt werden, daß wir hier von primitiven Bogen n-ter bzw. endlicher bzw. unendlicher Ordnung sprechen, ohne uns zunächst darum zu kümmern, für welche Ordnungen solche primitive Bogen wirklich existieren; im Verlaufe der Untersuchung wird sich indes zeigen, daß in der Ebene, außer den Konvexbogen, primitive Bogen nur noch von unendlicher Ordnung möglich sind (vgl. 3,1).

Besitzen alle Punkte eines Bogens $\mathfrak{B}$ *die gleiche Ordnung, so ist* $\mathfrak{B}$ *darstellbar als Summe endlich vieler primitiver Bogen von eben dieser Ordnung.*

Darüber hinaus gilt der folgende Zerlegungssatz:

2,7. *Zerlegungssatz: Jeder Bogen ist als abgeschlossene Summe von primitiven Bogen darstellbar.*

Der Beweis ergibt sich durch Anwendung von Nr. 2,5. Zunächst ist nämlich der Satz richtig, falls die Punkte höchstens zweiter Ordnung auf dem betrachteten Bogen $\mathfrak{B}$ überall dicht d. h. falls die Punkte mindestens dritter Ordnung nirgends dicht auf $\mathfrak{B}$ liegen; denn zufolge Nr. 2,5 ist alsdann $\mathfrak{B}$ abgeschlossene Summe von Konvexbogen und letztere sind alle primitiv. Wir wenden vollständige Induktion an, setzen also voraus, der Satz sei richtig, falls die Punkte höchstens $(n-1)$-ter Ordnung überall dicht auf $\mathfrak{B}$ liegen. Liegen nun die Punkte höchstens n-ter Ordnung überall dicht (d. h. also: Liegen die Punkte mindestens $(n+1)$-ter Ordnung nirgends dicht), so ist zufolge Nr. 2,5 der Bogen $\mathfrak{B}$ abgeschlossene Summe von Bogen $\mathfrak{T}_\nu$, deren jeder höchstens von n-ter Ordnung ist. Die $\mathfrak{T}_\nu$ sind nun einzeln zu untersuchen. Dabei können wir von dem Falle absehen, daß auf $\mathfrak{T}_\nu$ die Punkte höchstens $(n-1)$-ter Ordnung überall dicht liegen, weil alsdann für $\mathfrak{T}_\nu$ der Zerlegungssatz bereits als richtig bekannt ist. Wir nehmen also an, es existiere auf $\mathfrak{T}_\nu$ (mindestens) eine offene Teilmenge $\mathfrak{T}'_\nu$ von der Art, daß auf $\mathfrak{T}'_\nu$ Punkte n-ter Ordnung überall dicht liegen. Die Vereinigungsmenge O_ν aller solcher $\mathfrak{T}'_\nu$ ist eine in $\mathfrak{T}_\nu$ offene Menge, in welcher Punkte n-ter Ordnung überall dicht liegen und welche überdies keine Punkte höherer als n-ter Ordnung enthält. Daher sind alle Punkte aus O_ν von n-ter Ordnung (vgl. Nr. 2,4). Stellen wir nun O_ν als Vereinigung von (abzählbar unendlich vielen) abgeschlossenen Teilbogen $\mathfrak{T}'_{\nu\varrho}$ ($\varrho = 1, 2, \ldots$) dar, welche paarweise höchstens Randstellen gemeinsam haben, so ist jeder $\mathfrak{T}'_{\nu\varrho}$ Summe von (endlich vielen) primitiven Bogen n-ter Ordnung $\mathfrak{T}''_{\nu\tau}$ (gemäß Nr. 2, 6). Mithin ist die abgeschlossene Hülle $\bar{O}_\nu$ von O_ν darstellbar als abgeschlossene Summe der primitiven Bogen $\mathfrak{T}''_{\nu\tau}$. Nun handelt es sich noch um die Zerlegung des auf $\mathfrak{T}_\nu$ offenen Komplementes $R_\nu = \mathfrak{T}_\nu - \bar{O}_\nu$ von $\bar{O}_\nu$ in primitive Bogen. Ist R_ν nicht leer, so stelle man die offene Menge R_ν als Vereinigung von (abzählbar unendlich vielen) abgeschlossenen Teilbogen $\bar{\mathfrak{T}}_{\nu\varrho}$ dar, welche paarweise höchstens Randstellen gemeinsam haben. Auf R_ν und mithin auf $\bar{\mathfrak{T}}_{\nu\varrho}$ liegen aber die Punkte höchstens $(n-1)$-ter Ordnung überall dicht, so daß für $\bar{\mathfrak{T}}_{\nu\varrho}$ bereits der Zerlegungssatz gesichert ist. Der Zerlegungssatz gilt somit für jedes $\mathfrak{T}_\nu$, also auch für $\mathfrak{B}$, w. z. z. w.

Damit ist der Zerlegungssatz für Bogen beschränkter Ordnung bewiesen. Und daraus folgt (wegen Nr. 2,5) seine Gültigkeit auch für den Fall, daß die Punkte mindestens endlicher Ordnung nirgends dicht liegen.

Im Falle die Punkte unendlicher Ordnung nirgends dicht liegen sowie schließlich im Falle eines beliebigen Bogens führt dann wieder das Induktionsverfahren zum Ziel, wie es oben im Falle der Bogen beschränkter Ordnung angewandt wurde.

Zusatz: Aus dem vorstehenden Beweise folgt übrigens:

Damit $\mathfrak{B}$ abgeschlossene Summe von primitiven Bogen höchstens n-ter Ordnung (bzw. höchstens endlicher Ordnung) sei, ist notwendig und hinreichend, daß auf $\mathfrak{B}$ die Punkte mindestens $(n+1)$-ter Ordnung (bzw. unendlicher Ordnung) nirgends dicht liegen.

Man vergleiche dazu die genauere Aussage für ebene Bogen in Nr. 3,2.

2,8. Folgende Eigenschaft der primitiven Bogen mag noch Erwähnung finden, da sie später gebraucht wird:

Es sei $\mathfrak{P}$ ein primitiver Bogen n-ter Ordnung. Bezeichnen wir jede Sekante n-ter Ordnung an $\mathfrak{P}$ als eine *Maximalsekante* von $\mathfrak{P}$, so läßt sich behaupten:

Auf einem primitiven Bogen $\mathfrak{P}$ von n-ter Ordnung $(n \geqq 2)$ gibt es eine überall dichte Menge von Punkten P der folgenden Beschaffenheit: Zu jeder beliebig kleinen $\mathfrak{U}(P;\mathfrak{P})$ existieren Maximalsekanten von $\mathfrak{P}$, welche zugleich Maximalsekanten von $\mathfrak{U}(P;\mathfrak{P})$ sind und durch den Punkt P hindurchgehen. Diese Maximalsekanten können übrigens so gewählt werden, daß auf ihnen nur Schnittpunkte auftreten.

Zum Beweise betrachten wir einen beliebigen offenen Teilbogen $\mathfrak{P}'$ von $\mathfrak{P}$. Jener ist ebenfalls primitiv, besitzt also eine Maximalsekante s'. Zufolge Nr. 1,1 Zusatz kann s' so gewählt werden, daß s' mit $\mathfrak{P}'$ genau n *Schnitt*punkte, etwa $Q_1, Q_2, \ldots$, gemeinsam hat. Da alle hinreichend benachbarten Parallelen von s' ebenfalls derartige Maximalsekanten liefern (vgl. Nr. 1,1) und da die Schnittpunkte der letzteren mit $\mathfrak{P}'$ benachbart sind zu $Q_1, Q_2, \ldots$, so folgt: Es gibt eine abgeschlossene $\bar{\mathfrak{U}}(Q_1;\mathfrak{P}')$ von der Eigenschaft, daß durch jeden Punkt des abgeschlossenen Teilbogens $\mathfrak{P}_1 = \bar{\mathfrak{U}}(Q_1;\mathfrak{P}')$ von $\mathfrak{P}$ eine Maximalsekante an $\mathfrak{P}'$ geht. Durch die gleichen Überlegungen, wie sie von $\mathfrak{P}$ zu $\mathfrak{P}_1$ führten, erhält man aus $\mathfrak{P}_1$ einen abgeschlossenen Teilbogen $\mathfrak{P}_2$ von der Eigenschaft, daß durch jeden Punkt von $\mathfrak{P}_2$ je eine Maximalsekante an $\mathfrak{P}'$ und an $\mathfrak{P}_1$ geht. Fortsetzung dieses Verfahrens liefert eine absteigende Folge abgeschlossener Teilbogen $\mathfrak{P}_\nu$, so daß durch jeden Punkt von $\mathfrak{P}_{\nu+1}$ je eine Maximalsekante an $\mathfrak{P}_1, \ldots, \mathfrak{P}_\nu$ geht. Jeder Punkt P des, sicher nicht leeren, Durchschnittes der $\mathfrak{P}_\nu$ hat mithin die in der obigen Behauptung genannte Eigenschaft. Da $\mathfrak{P}_1$ und somit auch P dem beliebig gewählten Teilbogen $\mathfrak{P}'$ von $\mathfrak{P}$ angehört, liegen die P tatsächlich überall dicht auf $\mathfrak{P}$, womit alles bewiesen ist.

1. *Zusatz*: Eine naheliegende Modifikation des Beweises ergibt z. B. sogar die Existenz einer auf $\mathfrak{P}$ überall dichten Menge von Punkten P von folgender Eigenschaft: Zu jeder beliebig kleinen rechtseitigen $\mathfrak{U}^+(P;\mathfrak{P})$ können durch P Maximalsekanten gezogen werden, welche mit dem ganzen, rechts von P gelegenen Bogen genau zwei, zu $\mathfrak{U}^+(P;\mathfrak{P})$ gehörige *Schnitt*punkte gemeinsam haben und außerdem mit $\mathfrak{P}$ jedenfalls den *Schnitt*punkt P; natürlich ist *hier $n \geqq 3$ vorausgesetzt.* Man braucht nämlich im obigen Beweise an Stelle von Q_1 immer nur Q_3 der Betrachtung zugrunde zu legen (wobei angenommen ist, daß Q_1 und Q_2 rechts von Q_3 liegen).

2. *Zusatz*: Die im 1. Zusatz für primitive Bogen n-ter Ordnung aufgestellte Behauptung gilt auch für *primitive Bogen endlicher Ordnung.*

3. Primitive Bogen speziell in der Ebene.

3,1. Wir untersuchen nun die primitiven Bogen speziell in der Ebene noch näher. Hierbei ergibt sich nun folgende Tatsache: *Jeder ebene primitive Bogen ist entweder von zweiter oder von unendlicher Ordnung. Von Strecken ist dabei, wie immer, abgesehen.*

Der Beweis ist erbracht, falls gezeigt wird, daß Punkte P von der in Nr. 2,8, 1. und 2. Zusatz, genannten Beschaffenheit nicht existieren. Um dies einzusehen, betrachten wir einen derartigen Punkt P auf dem (primitiven) Bogen $\mathfrak{P}$, dessen Ordnung weder zwei

noch unendlich sein möge. Ohne Beschränkung der Allgemeinheit kann P als *innerer* Punkt von $\mathfrak{P}$ angenommen werden. Ferner sei $\mathfrak{U}^+$ eine rechtsseitige Umgebung von P auf $\mathfrak{P}$ und s_1 eine Sekante durch P, welche mit $\mathfrak{U}^+$ außerdem die Schnittpunkte Q_1 und R_1 und keine weiteren gemeinsam hat. Der Natur der Sache nach kann übrigens s_1 durch die, Q_1 und R_1 enthaltende, orientierte Halbgerade mit P als Anfangspunkt ersetzt und damit der Begriff „rechte" bzw. „linke Seite von s_1" eindeutig erklärt werden, was für die folgenden Überlegungen bequem ist. Es sei nun Q_1 der erste auf $\mathfrak{P}$ rechts von P gelegene Schnittpunkt von s_1 mit $\mathfrak{P}$. Dann verläuft der Teilbogen $\overset{\frown}{PQ_1}$ von $\mathfrak{P}$, dessen Randpunkte P und Q_1 sind, ganz auf der *einen*, etwa der *linken* Seite von s_1 (d. h. in der links von s_1 gelegenen abgeschlossenen Halbebene). Durch P können wir jetzt (nach Voraussetzung) eine neue orientierte Halbgerade s_2 ziehen, welche mit $\overset{\frown}{PQ_1}$, außer P, die (von P und Q_1 verschiedenen) Schnittpunkte Q_2 und R_2 gemeinsam hat und mit $\mathfrak{U}^+$ keine weiteren Punkte; übrigens möge Q_2 auf $\mathfrak{P}$ rechts von P und R_2 rechts von Q_2 liegen. Da nur *Schnitt*punkte auftreten, so liegt $\overset{\frown}{PQ_2}$ auf der gleichen Seite von s_2 wie $\overset{\frown}{R_2Q_1}$. Und zwar kann $\overset{\frown}{PQ_2}$ nur auf der *rechten* Seite von s_2 liegen; denn Q_1 liegt gewiß auf der rechten Seite von s_2, da s_2 auf der linken Seite von s_1 verläuft. Wir ziehen schließlich durch P eine dritte orientierte Halbgerade s_3, welche mit $\overset{\frown}{PQ_2}$, abgesehen von P, die (von P und Q_2 verschiedenen) Schnittpunkte Q_3 und R_3 gemeinsam hat, wobei Q_3 auf $\mathfrak{P}$ links von R_3 liegen möge; nach Voraussetzung kann übrigens s_3 so gewählt werden, daß s_3 außer P, Q_3, R_3 keine Punkte mit $\mathfrak{U}^+$ gemeinsam hat. Da $\overset{\frown}{PQ_2}$ auf der rechten Seite von s_2 liegt, so muß s_3 auf der rechten Seite von s_2 verlaufen. Andererseits verläuft aber s_3 auf der linken Seite von s_1, muß daher, außer den auf $\overset{\frown}{PQ_2}$ liegenden Punkten P, Q_3, R_3, noch mindestens einen Punkt mit $\overset{\frown}{R_2Q_1}$ also mit $\mathfrak{U}^+$ gemeinsam haben. In der Tat: Sämtliche Punkte des Bogens $\overset{\frown}{R_2Q_1}$ liegen zugleich auf der linken Seite von s_1 und auf der rechten Seite von s_2. Daher muß jede Halbgerade durch P, die links von s_1 und rechts von s_2 verläuft, den Teilbogen $\overset{\frown}{R_2Q_1}$ treffen.

Damit sind wir bereits beim angekündigten Widerspruch angelangt, w. z. z. w.

1. *Zusatz*: Daß die Konvexbogen mit den (ebenen) primitiven Bogen zweiter Ordnung sich decken, wurde schon früher bemerkt. Die *Existenz primitiver Bogen unendlicher Ordnung* beweist man etwa auf Grund der Bemerkung, daß jeder Konvexbogen (oder allgemeiner jeder Bogen beschränkter oder endlicher Ordnung) überall vorn und hinten differenzierbar sein muß [16]). Bezeichnet also $y = f(x)$ eine eindeutige stetige Funktion, welche nirgends weder eine vordere noch eine hintere Ableitung besitzt, so hat der einfache Bogen $x = t$, $y = f(t)$ nirgends vordere oder hintere Tangenten, enthält also keinen konvexen Teilbogen und folglich keine Punkte beschränkter oder endlicher Ordnung. Beispiele von primitiven Bogen unendlicher Ordnung, die *sogar gewöhnliche Bogen* sind, hat Herr Hjelmslev [17]) angegeben, indem er die Tatsache benützt, daß bei einem gewöhnlichen Konvexbogen fast überall die zweiten Ableitungen vorhanden sind.

2. *Zusatz*: Daß primitive Bogen $2n$-ter Ordnung $(n \geqq 2)$ nicht existieren, folgt übrigens unmittelbar aus der Bemerkung, daß jeder Punkt $2n$-ter Ordnung auf einem Bogen $\mathfrak{B}$ der gleichen Ordnung $2n$ zur Begrenzung der konvexen Hülle von $\mathfrak{B}$ gehört.

3,2. Zufolge Nr. 3,1 ergibt jetzt der Zerlegungssatz von Nr. 2,7: *Jeder ebene Bogen ist abgeschlossene Summe von Strecken, Konvexbogen und von primitiven Bogen unendlicher Ordnung.*

---

[16]) Vgl. etwa [4]) a. a. O., Nr. 38.

[17]) Siehe [1]) a. a. O., Seite 482.

Ferner ergibt der Zusatz zu Nr. 2,7:

Damit $\mathfrak{B}$ abgeschlossene Summe von Strecken und Konvexbogen sei, ist notwendig und hinreichend, daß auf $\mathfrak{B}$ die Punkte unendlicher Ordnung nirgends dicht liegen.

Speziell: *Jeder Bogen endlicher Ordnung ist abgeschlossene Summe von Strecken und Konvexbogen.*

Zusatz: Ein ebener Bogen (*ohne Strecken*) ist dann (und nur dann) primitiv von unendlicher Ordnung, wenn er keine konvexen Teilbogen enthält.

3,3. Die Bogen endlicher Ordnung sind zufolge Nr. 2,2 dadurch charakterisiert, daß sie keine Punkte unendlicher Ordnung enthalten. Eine andere Kennzeichnung ist die folgende: Jeder Bogen endlicher Ordnung ist überall vorn und hinten differenzierbar [16]) und von endlichem Vielfachheitsgrad, d. h. er enthält keine Punkte von unendlicher Vielfachheit; diese Bedingung ist also jedenfalls notwendig. Andererseits sind bei einem überall vorn und hinten differenzierbaren Bogen von endlichem Vielfachheitsgrad die Sekanten von unendlicher Ordnung dadurch charakterisiert, daß sie in mindestens einem Punkte B vordere oder hintere Tangenten des Bogens sind, welche mit dem Bogen unendlich viele, vom Berührpunkt getrennt gelegene Punkte gemeinsam haben und wobei der Berührungspunkt B Häufungspunkt jener Punkte ist. Bezeichnen wir daher [18]) einen solchen Punkt B als „(vorderen bzw. hinteren) *Undulationspunkt*“ von $\mathfrak{B}$, so können wir sagen:

Ein Bogen besitzt dann und nur dann endliche Ordnung, wenn er von endlichem Vielfachheitsgrad und in jedem Punkte vorn und hinten differenzierbar ist und wenn er keine Undulationspunkte aufweist. Liegen hingegen die Undulationspunkte überall dicht, so enthält der Bogen keinen konvexen Teilbogen.

---

[18]) Vgl. [1]) a. a. O., Seite 449.

Erlangen, Mathematisches Seminar, 30. September 1930.

Eingegangen 4. Oktober 1930.

Einfacher Beweis eines Satzes von Kronecker.

Von *A. Korselt* in Plauen i. V.

Der Satz lautet: *Eine unzyklische Abelsche Gruppe ist das direkte Produkt von unabhängigen zyklischen Gruppen.*

Ich beweise diesen Satz noch einfacher als Mathewson in Band 161, Heft 4 dieser Zeitschrift, indem ich nicht die umständliche Lehre von den Quotientengruppen und deren Isomorphien brauche, auch nicht die Gruppe in einartige (mit Primpotenz-Ordnung) zerlege und mich nur auf gewisse Beschaffenheiten endlicher Mengen beziehe.

1. Es sei G irgendeine endliche Gruppe, t ein Teil von G. t heiße *Unterbau* (Basis) von G, wenn t in keinem Unterteiler von G liegt. Dann wird G „durch t erzeugt, bestimmt oder aufgespannt".

2. *Marke von G oder t* = Operator von G bezw. t.

3. *Beziehung von oder für t* = Gleichung von der Form $a_1^{\lambda_1} \cdots a_n^{\lambda_n} = 1$, worin die a_ν Marken aus t und die Höhen λ_ν ganze Zahlen sind.

a ist freie Marke von t, wenn jede sie erwähnende Beziehung zwischen Marken aus t richtig bleibt, falls man a durch 1 ersetzt. Andernfalls ist *a gebundene Marke aus t.*

4. *Dehnung von t* = Anzahl der gebundenen Marken von t.

$L(t)$ sei das All der Beziehungen zwischen Marken aus t. *Gewicht von $L(t)$* = niedrigster unter den Beträgen der fülligen Höhen, die als Exponenten von gebundenen Marken von t in $L(t)$ auftreten.

5. Jede endliche Gruppe hat offenbar Unterbauten (Basen) von möglichst niedriger Dehnung und unter diesen solche von möglichst kleinem Gewichte.

6. Nun sei A eine endliche Abelsche Gruppe. Sie hat einen Unterbau, der gebundene Marken enthält, z. B. ist A selbst ein solcher. Also auch einen solchen $t \equiv (a_1, a_2, \ldots, a_n)$ von niedrigster *fülliger* Dehnung d und sogar von niedrigstem Gewicht g. Also etwa die gebundene Marke a_1 kommt in $L(t)$ mit der Höhe g vor, es sei z. B.

$$a_1^{m_1} \cdots a_p^{m_p} = 1, \tag{a}$$

eine Beziehung aus $L(t)$, mit

$$m_\pi \text{ ganz}, \quad m_1 = g. \tag{b}$$

Ich setze

$$m_2 = m_1 q_2 + r_2, \ldots, m_p = m_1 q_p + r_p, \tag{c}$$

$$q_\pi \text{ ganze Zahl}, \quad 0 \leqq r_\pi < m_1 = g. \tag{d}$$

$$a_1 a_2^{q_2} \cdots a_p^{q_p} = a_1', \tag{e}$$

so daß nun

$$a_1'^{g} a_2^{r_2} \cdots a_p^{r_p} = 1. \tag{f}$$

Offenbar ist dann auch $t' \equiv (a_1', a_2, \ldots, a_n)$ ein Unterbau von A. Aber a_1' kommt in $L(t')$ nur mit Höhen vor, die Vielfache von g sind. Eine niedrigere Potenz als $a_1'^{g}$

kann nicht auftreten, weil man durch Wiedereinsetzung des Wertes von a_1' aus e) gegen Voraussetzung den Unterbau t als von kleinerem Gewichte als g erkennen würde. Wären von den Zahlen r_π einige positiv (nicht bloß *mild* natürlich), so hätte nach d) t' ein niedrigeres Gewicht als t, was nicht sein soll.

Daher ist

g) $$r_\pi = 0, \quad a_1'^g = 1.$$

Nach dem oben Gesagten muß nun a_1' freie Marke von t' sein, und t' hat eine geringere Dehnung als t. Da aber t schon die *niedrigste füllige* Dehnung hatte, so besitzt t' keine *füllige* Dehnung d', sondern es ist $d' = 0$, d. h. es kommen in t' keine gebundenen Marken mehr vor, t' ist „freier oder unabhängiger Unterbau von A“, und jede Beziehung $a_1^{s_1} a_2^{s_2} \cdots a_n^{s_n} = 1$ hat als Folge $a_1^{s_1} = a_2^{s_2} = \cdots = a_n^{s_n} = 1$, A ist in die unabhängigen Zyklen (a_1'), (a_2), . . ., (a_n) zerlegt, was zu beweisen war.

Ist A einartig und zyklisch, so enthält t' nur die Marke a_1', man hat ein „uneigentliches Produkt“.

7. Auf ähnliche Art leitet man durch einen fast reinen Bestandsbeweis die übrigen bekannten Eigenschaften der Basen von Abelschen Gruppen ab. Ist z. B. a ein Glied einer unabhängigen Basis oder überhaupt einer Basis, $a = a_1 a_2$, sind die Ordnungen von a_1 und a_2 fremd, so kann man a weglassen und dafür a_1, a_2 setzen, und umgekehrt, ohne die Unabhängigkeit des Unterbaues zu stören.

Plauen, den 18. Januar 1930.

Eingegangen 22. Januar 1930.

Zur vorstehenden Arbeit von Herrn A. Korselt.

Von *Wolfgang Franz* in Marburg.

Der neue kurze Korseltsche Beweis des Satzes, daß *jede endliche Abelsche Gruppe direktes Produkt zyklischer Gruppen* ist, lautet in der üblichen mathematischen Terminologie folgendermaßen:

Unter allen erzeugenden Elementsystemen für die Gruppe betrachte man diejenigen, bei denen die Anzahl der in einer Relation

$$A_1^{x_1} A_2^{x_2} \cdots A_r^{x_r} = E \text{ mit } A_1^{x_1} \neq E, \ldots, A_r^{x_r} \neq E$$

auftretenden Elemente positiv aber minimal ist, und unter diesen ein solches, bei dem der kleinste Betrag der auftretenden Exponenten $x_1, \ldots, x_r$ minimal ist. Die obige Relation sei bereits aus einem in dieser Weise gewählten System so ausgewählt, daß x_1 jener dem Betrage nach kleinste Exponent ist. Dann dividiere man mit Rest:

$$x_i = x_1 q_i + r_i \quad \text{für } i = 2, \ldots, r \quad (0 \leqq r_i < |x_1|)$$

und ersetze in dem oben betrachteten System A_1 durch $\bar{A}_1 = A_1 A_2^{q_1} \cdots A_r^{q_r}$. Man erkennt sofort, daß auch das neue System die Gruppe erzeugt, daß die Zahl der in einer Relation der betrachteten Art auftretenden Elemente im neuen System nicht größer geworden sein kann, und endlich, wegen der Minimumseigenschaft von x_1, daß $\bar{A}_1$ in allen solchen Relationen nur als Potenz von $\bar{A}_1^{r_1}$ auftreten kann. Die obige Relation geht jetzt über in

$$A_1^{x_1} A_2^{r_2} \cdots A_r^{r_r} = E,$$

und aus der Minimumseigenschaft von x_1 und den Ungleichungen folgt $r_2 = \cdots = r_r = 0$, also $\bar{A}_1^{x_1} = E$. Daher tritt im neuen System $\bar{A}_1$ in solchen Relationen garnicht auf, die Anzahl der in solchen Relationen auftretenden Elemente ist also sogar kleiner geworden. Das heißt aber nach der ersten Minimumsforderung, daß solche Relationen beim neuen System überhaupt nicht auftreten, so daß die Gruppe also direktes Produkt der durch diese Elemente gelieferten zyklischen Gruppen ist.

Eingegangen am 1. Juli 1930.

Gewindebüschel und ihre Invarianten.

Von *Frank Löbell* in Stuttgart.

Im folgenden sollen nur die Haupteigenschaften der Büschel reeller linearer Komplexe entwickelt werden; es wird sich also um sachlich Bekanntes handeln [1]), aber man wird bemerken, daß die Verwendung der Schraubenrechnung [2]) eine sowohl formale wie gedankliche Vereinfachung der Theorie ermöglicht.

Es seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei Schrauben, für die $\overline{\mathfrak{a} \times \mathfrak{b}} \neq 0$ ist, die also eigentliche, nicht parallele Achsen haben; ihr gemeinsames Lot ist die Achse c der Schraube $\mathfrak{a} \times \mathfrak{b}$. Die Mannigfaltigkeit der Schrauben

$$\mathfrak{x} = \lambda \mathfrak{a} + \mu \mathfrak{b},$$

wo λ und μ unabhängig voneinander alle nicht-dualen Zahlen durchlaufen, besteht aus lauter Schrauben, deren Achsen von c senkrecht geschnitten werden; denn es ist $\mathfrak{a}\mathfrak{b}\mathfrak{x} = 0$. Zwei Schrauben $\mathfrak{x}$, für die das Verhältnis $\lambda : \mu$ denselben Wert hat, haben eine gemeinsame Achse und gleichen Parameter. Die Achsen aller Schrauben $\mathfrak{x}$ bilden daher eine Regelschar, die sog. Achsenfläche der Schraubenmannigfaltigkeit. Eine Menge von Schrauben mit gemeinsamer Achse und gleichem Parameter repräsentiert ein Gewinde; demgemäß stellt die Gesamtheit der Schrauben $\mathfrak{x}$ ein „Gewindebüschel" dar. Jedes Gewinde mit eigentlicher Achse kann offenbar auf zwei Arten durch einen dualen Vektor abgebildet werden, dessen erster Teil ein Einheitsvektor ist.

Es soll die Gestalt der Achsenfläche und die Verteilung der Parameterwerte der Gewinde des Büschels über die Schar ihrer Erzeugenden hin untersucht werden.

Da die Achsen der Schrauben $\mathfrak{x}$ den Vektoren des Büschels $\lambda \bar{\mathfrak{a}} + \mu \bar{\mathfrak{b}}$ parallel sind, so kann man zu jeder dieser Schrauben eine solche mit senkrechter Achse finden; wir dürfen deshalb annehmen, daß schon $\mathfrak{a}$ und $\mathfrak{b}$ senkrechte Achsen haben, d. h. daß $\overline{\mathfrak{a}\mathfrak{b}} = 0$ ist, und es sei ferner $\bar{\mathfrak{a}}^2 = \bar{\mathfrak{b}}^2 = 1$. Es ist weiterhin bequem, das Gewindebüschel in der Form darzustellen:

---

[1]) Es sei nur hingewiesen auf die Arbeiten von W. Fr. Meyer, Über die Achsenfläche eines Büschels linearer Komplexe ..., dieses Journal **159** (1928), S. 50 ff., und von K. Kommerell, Über die Zentralachsen eines Büschels von Dynamen ..., dieses Journal **161** (1929), S. 113 ff., sowie auf die dort angeführte Literatur; besonders beachte man auch die äußerst kurze Behandlung des Gewindebüschels mit Hilfe Graßmannscher Methoden bei A. Lotze, Die Grundgleichungen der Mechanik (Leipzig 1922), S. 48 ff.

[2]) Der hier benützte, auf Clifford und Study zurückgehende Kalkül der dualen Vektoren ist auseinandergesetzt in Blaschkes Vorl. ü. Differentialgeometrie I, 3. Aufl. (Berlin 1930) S. 261 ff. (1. Aufl. S. 190 ff., 2. Aufl. S. 191 ff.); ferner in einem Beitrag des Verfassers zur Festschrift der Techn. Hochsch. Stuttgart (Berlin 1929), S. 210 ff. Es könnte auch die Punktrechnung oder die Motorrechnung angewandt werden; s. v. Mises, Motorrechnung, ein neues Hilfsmittel der Mechanik, Zeitschr. f. ang. Math. u. Mech. **4** (1924), S. 155 ff., und Lotze, Punkt- und Vektorrechnung (Berlin und Leipzig 1929).

Die dualen Vektoren werden hier mit deutschen Buchstaben bezeichnet; ist A irgendeine duale Größe, so bedeute $\bar{A}$ ihren „ersten Teil", der von dem Faktor ε, der dualen Einheit, frei ist, $\bar{\bar{A}}$ ihren „zweiten Teil", der mit dem Faktor ε behaftet ist: $A = \bar{A} + \varepsilon \bar{\bar{A}}$.

$$\mathfrak{x} = \mathfrak{a}\cos\xi + \mathfrak{b}\sin\xi,$$

wo ξ die nicht-dualen Zahlen des Intervalls $\langle 0, \pi)$ durchlaufe.

Um den Parameter p von $\mathfrak{x}$ zu bestimmen, quadrieren wir $\mathfrak{x}$. Denn weil der Parameter einer Schraube gleich dem Verhältnis des zweiten Teils ihrer dualen Länge zu deren erstem Teil ist, so ist wegen $\bar{\mathfrak{x}}^2 = 1$ $2p = \overline{\overline{\mathfrak{x}^2}}$, und ebenso sind $p' = \frac{1}{2}\overline{\overline{\mathfrak{a}^2}}$ und $p'' = \frac{1}{2}\overline{\overline{\mathfrak{b}^2}}$ die Parameter von $\mathfrak{a}$ und $\mathfrak{b}$; ferner gilt für den kürzesten Abstand $2d_0$ der Achsen von $\mathfrak{a}$ und $\mathfrak{b}$, da der duale Winkel dieser Schrauben $\frac{\pi}{2} + \varepsilon \cdot 2d_0$ ist, $2d_0 = -\overline{\overline{\mathfrak{a}\mathfrak{b}}}$. Folglich führt die Gleichung

$$\mathfrak{x}^2 = \mathfrak{a}^2\cos^2\xi + \mathfrak{b}^2\sin^2\xi + 2\,\mathfrak{a}\mathfrak{b}\cos\xi\sin\xi$$

unmittelbar auf die Beziehung:

$$p = p'\cos^2\xi + p''\sin^2\xi - 2d_0\cos\xi\sin\xi.$$

Wir betrachten außer $\mathfrak{x}$ noch die Schraube

$$\mathfrak{x}' = \mathfrak{a}\sin\xi - \mathfrak{b}\cos\xi,$$

die dasjenige Gewinde des Büschels darstellt, dessen Achse zu der von $\mathfrak{x}$ lotrecht gerichtet ist. Wir suchen den Abstand $2d$ der Achsen von $\mathfrak{x}$ und $\mathfrak{x}'$; zu dem Zweck bilden wir, da $2d = -\overline{\overline{\mathfrak{x}\mathfrak{x}'}}$ ist, das skalare Produkt von $\mathfrak{x}$ und $\mathfrak{x}'$. Aus

$$\mathfrak{x}\mathfrak{x}' = (\mathfrak{a}^2 - \mathfrak{b}^2)\cos\xi\sin\xi - \mathfrak{a}\mathfrak{b}(\cos^2\xi - \sin^2\xi)$$

lesen wir somit unmittelbar ab:

$$d = (p'' - p')\cos\xi\sin\xi - d_0(\cos^2\xi - \sin^2\xi);$$

da die Drehung um $\frac{\pi}{2}$, die die positive Achsenrichtung von $\mathfrak{x}'$ in die von $\mathfrak{x}$ überführt, im gleichen Sinn erfolgt wie die Drehung um $\frac{\pi}{2}$, die die positive Achsenrichtung von $\mathfrak{a}$ in die von $\mathfrak{b}$ verwandelt, so ergibt sich d als positive Zahl, wenn die Verschiebung, die mit dieser Drehung verbunden werden muß, damit die Achse von $\mathfrak{x}'$ mit der von $\mathfrak{x}$ zusammenfällt, die Richtung der Achse von $\mathfrak{a}\times\mathfrak{b}$ hat.

Die letzte Gleichung zeigt, daß man immer den Winkel ξ so wählen kann, daß d verschwindet, und zwar im allgemeinen auf genau eine Weise, im besonderen auf unendlich viele Arten. Es darf deshalb fernerhin angenommen werden, daß schon $\mathfrak{a}$ und $\mathfrak{b}$ als ein Paar von Schrauben ausgesucht waren, deren Achsen sich senkrecht schneiden, für die also $\mathfrak{a}\mathfrak{b} = 0$, insbesondere $d_0 = 0$ ist. Bedeuten p_1 und p_2 die Parameter dieser Schrauben, so gilt also [3]):

$$p = p_1\cos^2\xi + p_2\sin^2\xi, \tag{1}$$

$$d = \tfrac{1}{2}(p_2 - p_1)\sin 2\xi. \tag{2}$$

Die Formel (1) gibt das Gesetz der Verteilung der Parameter der Gewinde des Büschels über die Achsenfläche; (2) zeigt, daß diese eine Studysche Strahlenkette [4]), d. h. ein Zylindroid oder speziell eine Ebene ist, wenn man nur noch bewiesen hat, daß d der kürzeste Abstand der Achse von $\mathfrak{x}$ von dem Schnittpunkt C der Achsen von $\mathfrak{a}$ und $\mathfrak{b}$ ist:

Wenn $A = \bar{A} + \varepsilon\bar{\bar{A}}$ irgend eine duale Größe vorstellt, so bezeichne $\tilde{A}$ die zu ihr „konjugierte“: $\tilde{A} = \bar{A} - \varepsilon\bar{\bar{A}}$. — Es bedeute $\mathfrak{a}_0$ die Einheitsschraube von $\mathfrak{a}$, $\mathfrak{b}_0$ die von $\mathfrak{b}$, und es sei $a = 1 + \varepsilon p_1$, $b = 1 + \varepsilon p_2$, so daß $\mathfrak{a} = a\mathfrak{a}_0$, $\mathfrak{b} = b\mathfrak{b}_0$ ist. Die Vierteldrehung um c, die $\mathfrak{a}_0$ in $\mathfrak{b}_0$, $\mathfrak{b}_0$ in $-\mathfrak{a}_0$ überführt, ändert $\mathfrak{x} = a\mathfrak{a}_0\cos\xi + b\mathfrak{b}_0\sin\xi$ in

[3]) Die Formeln von Hamilton und Mannheim in der Theorie der Strahlensysteme (s. Blaschke l. c. S. 283 f.) hängen ersichtlich eng mit (2) und (1) zusammen.

[4]) Siehe E. Study, Geometrie der Dynamen (Leipzig 1903), S. 320.

$\mathfrak{y} = a\mathfrak{b}_0 \cos\xi - b\mathfrak{a}_0 \sin\xi$ um. Da bei einer Umlegung der Parameter jedes Gewindes sein Vorzeichen wechselt, so verwandelt die Spiegelung an C, weil sie die Schrauben $\mathfrak{a}_0$ und $\mathfrak{b}_0$ in $\pm\mathfrak{a}_0$ und $\pm\mathfrak{b}_0$ überführt (je nachdem man sie als Repräsentanten eines Geschwindigkeitszustandes oder eines Kräftesystemes auffaßt [1]), $\mathfrak{y}$ in $\mathfrak{z} = \pm\tilde{a}\mathfrak{b}_0 \cos\xi \mp \tilde{b}\mathfrak{a}_0 \sin\xi$; wegen $a\tilde{a} = b\tilde{b} = 1$ ist aber $\mathfrak{z} = \mp\tilde{a}\tilde{b}(a\mathfrak{a}_0 \sin\xi - b\mathfrak{b}_0 \cos\xi)$, d. h. durch die Aufeinanderfolge einer Vierteldrehung um c und der Spiegelung an C geht das Gewinde $\mathfrak{x}$ in $\widetilde{ab}\mathfrak{x}'$, die Achse von $\mathfrak{x}$ also in die von $\mathfrak{x}'$ über. Mithin fällt der Mittelpunkt des gemeinsamen Lotes dieser Achsen in den Punkt C, das Zentrum der Strahlenkette; dies war zu beweisen. — Bei dieser Überlegung wurde der Satz benützt, daß die Bewegung oder Umlegung, die die dualen Vektoren $\mathfrak{v}_i$ in $\mathfrak{v}_i^*$ und die dualen Zahlen ϱ_i in ϱ_i^* transformiert ($i = 1, 2, \ldots, n$), auch $\mathfrak{x} = \sum_{i=1}^{n} \varrho_i \mathfrak{v}_i$ in $\mathfrak{x}^* = \sum_{i=1}^{n} \varrho_i^* \mathfrak{v}_i^*$ transformiert, wobei die Schrauben $\mathfrak{v}_i$ beliebig sind; bei einer Bewegung gilt $\varrho^* = \varrho$, bei einer Umlegung $\varrho^* = \tilde{\varrho}$.

Die Relation (2) gibt in einfachster Weise über die Gestaltverhältnisse der Strahlenketten erschöpfenden Aufschluß und zeigt ohne weiteres, daß eine solche nach Form und Größe, d. h. bis auf ihre Lage im Raum, durch den Wert von $(p_2 - p_1)^2$ eindeutig bestimmt ist; geometrisch bedeutet $|p_2 - p_1|$, wenn es $\neq 0$ ist, den Abstand der beiden am weitesten voneinander entfernten Erzeugenden der Strahlenkette, deren Richtungen übrigens die Winkel der sich senkrecht schneidenden Achsen halbieren. Nach (1) sind p_1 und p_2 die Extreme aller im Gewindebüschel vorkommenden Parameterwerte; diese Bemerkung erschließt einen bekannten, einfachen Weg zur Berechnung der Parameter der beiden Gewinde mit lotrecht sich durchdringenden Achsen, der sog. Hauptgewinde, in einem gegebenen Büschel $\lambda\mathfrak{a} + \mu\mathfrak{b}$, wo $\mathfrak{a}$ und $\mathfrak{b}$ wieder wie anfangs beliebige Schrauben mit linear unabhängigen Achsenrichtungen sind, mittels der Jacobischen Form der beiden durch Zerlegung der quadratischen Form $(\lambda\mathfrak{a} + \mu\mathfrak{b})^2$ in ihren ersten und zweiten Teil entstehenden Formen.

Man erkennt nach diesen Ausführungen:

Die beiden nicht-dualen Größen [2])

$$h = \tfrac{1}{2}(p_1 + p_2) \quad \text{und} \quad k = p_1 \cdot p_2$$

bilden ein vollständiges System von Invarianten eines Gewindebüschels gegenüber der Gruppe der Bewegungen des euklidischen Raumes. Ein vollständiges Invariantensystem gegenüber der Gruppe der Bewegungen und Umlegungen wird von den Größen

$$j = \left(\frac{p_2 - p_1}{2}\right)^2 \quad \text{und} \quad k$$

gebildet.

Die einzige orthogonale Invariante der Strahlenkette ist

$$j = h^2 - k.$$

Die notwendige und hinreichende Bedingung dafür, daß die Strahlenkette ein ebenes Strahlenbüschel sei, ist $p_1 = p_2\,(= p)$ oder $j = 0$; ist sogar $h = k = 0$, so haben zudem alle Gewinde des Büschels verschwindende Parameter.

Ist $h \neq 0$, so gibt es zwei reell-getrennte, zusammenfallende oder imaginäre Gewinde mit verschwindendem Parameter, je nachdem $k \lessgtr 0$. Ist $k \neq 0$, aber $h = 0$, so kreuzen sich die Achsen der beiden alsdann existierenden reellen Gewinde mit verschwindenden Parametern senkrecht, ohne sich zu treffen; sie sind dann zugleich die Achsen größten gegenseitigen Abstands.

[1]) Vgl. F. Klein, Ges. math. Abh. I (Berlin 1921), S. 508.

[2]) Nach (1) kann natürlich statt $p_1 + p_2$ die Summe der Parameter irgend zweier Gewinde des Büschels mit zueinander senkrecht gerichteten Achsen genommen werden.

Eingegangen 9. Mai 1930.